

51. 中文發明說明書 (發明之名稱)

部，又，將存儲信息資料為壓縮資料及延長處理程序，或壓縮程序與組合，或再生裝置，形成可判定可適用於壓縮存儲信息的延長處理程序。

52. 系統結構圖 (發明之名稱)

本系統或設備中各組件與各組件 (CDS) 與 (S) 之關係圖

(發明之名稱)

53. 系統結構圖 (發明之名稱)

(發明之名稱)

五、發明說明 (1)

【發明所屬之技術領域】

本發明，係有關資料處理裝置及資料處理方法，更詳細而言，係有關用以構成資料存儲信息之資料的正當性，即用以驗證有無篡改之方法，裝置，賦予驗證之方法，又，有關在驗證處理時必要的控制邏輯，依該控制對於各個數據的主權範圍由進行生成，形成可視為安全之裝置及方法。又，本發明，係提供用以排除資料存儲信息之不當利用的構成，具體而言，係有關用以識別不當利用發生時並形成用以排除存儲信息之不當利用的裝置及方法。進而本發明，係有關於應利用資料處理裝置之存儲信息，及其他資料處理裝置中也可利用之存儲信息根據資料處理裝置固有之資訊等做為可容許進行設定之裝置及方法，進而，有關用以構成資料存儲信息之資料的正當性，即用以驗證有無篡改之方法，裝置，賦予驗證之方法。

進而，本發明，係有關資料處理裝置，存儲信息資料生成方法，及資料處理方法，將含聲音資訊，圖像資訊，程式資料至少其中之一資料加以數位化處理，並與各種之聲音資訊一起提供給存儲信息利用時，使存儲信息利用時再生，執行，或記錄裝置進行資料處理等之構成中，並提供存儲信息資料安全管理之基礎下用以實現形成可提供及利用之存儲信息資料構成。

進而，係有關資料處理裝置，資料處理方法及存儲信息資料生成方法，用以提供有效執行被壓縮資料存儲信息之聲音資料，或圖像資料等情形之再生處理的構成，具

本系統或設備中各組件與各組件 (CDS) 與 (S) 之關係圖

五、發明說明 (2)

體而言，係將存儲信息資料之構成做為組合壓縮資料及延長處理程序之構成，或將適用延長處理程序後含聲音資訊並根據進行控制之壓縮資料存儲信息的裝置與利用以將資料輸出可適用之延長處理程序做為可用以執行再生處理。

本發明，係有關 DVD，CD 等之記憶裝置，或 CATV，網路網路，衛星通訊等以有線，無線各種裝置等之網路所取得之聲音，圖像，遊戲，程式等之各種存儲信息，在使用者之所有的記錄再生係中進行再生，並存儲於專用記憶裝置，譬如記憶卡，硬碟，CD-R 等，同時利用被存儲於記憶裝置之存儲信息，用以實現利用存儲信息記錄之希望的限制利用之構成，同時將該被記之存儲信息，在正規使用者以外之第三者不該不當利用及用以確保安全之構成及方法。

【先前之技術】

最近，遊戲程序，聲音數據，圖像數據，文書作成程式等，使各個軟體資料 (以下，將此等稱為存儲信息 (Content))，透過網路等之網路，或透過 DVD，CD 等之可記錄的記憶媒體進行流通，此等之流通存儲信息，係使用者所有之 Personal Computer)，附屬於遊戲機等之記錄再生機體的記錄裝置，譬如可容納於記憶卡，硬碟等，一旦被容納之後，係由容納媒體經由再生形成可利用。

譬如技術之影響遊戲機，PC 等之資訊機器中被使

(發明之名稱)

54. 系統結構圖 (發明之名稱)

(發明之名稱)

本系統或設備中各組件與各組件 (CDS) 與 (S) 之關係圖

- 5 -

五、發明說明 (3)

用記錄卡裝置之主要構成要素，係具有：控制裝置，為了動作控制；連接器，被連接於控制裝置並為了連接於被設在資訊機器本體的切接；及非易失性記憶體，被連接於控制裝置並為了用以記憶資料，與關於記憶卡之非易失性記憶體係經由 E P R O M，閃光記憶體等被構成。

被記錄於如此之記憶卡之資料，或程式等之各種的存儲信息，係做為再生機體被利用由遊戲機，PC 等之資訊機器本體由使用者來，或透過被連接之輸入裝置的使用者之指示由非易失性記憶體被利用，並透過資訊機器本體，或被連接之顯示部，揚聲器等被再生。

遊戲程序，音樂數據，圖像數據等，多數之軟體，存儲信息，一般均係在其作成者，販賣者被保有版權等，因此，在此等之存儲信息的配布時，係固定之限制利用，即僅對正規之使用者，許可軟體之使用，使使求許可複製等不能進行，即形成一般性的採用考慮安全之構成。

對使用者用以實現限制利用之 1 種方法，係配布存儲信息的暗號化處理，即，譬如透過網路網路等用以配布暗號化之聲音資料，圖像資料，遊戲程序等之各種存儲信息，同時對該暗號正正規使用的人，用以譯碼配布之暗號化存儲信息的裝置，即賦予譯碼暗號之構成。

暗號化資料，係根據指定之字樣經由譯碼化處理可回到可利用之譯碼資料，在如此之資訊的暗號化處理使用暗號化暗號，在重號化處理使用譯碼化暗號之資料暗號化，譯碼化方法係由先前即為眾所周知。

本系統或設備中各組件與各組件 (CDS) 與 (S) 之關係圖

- 6 -

五、發明說明(4)

在使用暗號化論點及譯碼化論點之資料暗號化、譯碼化方法之態樣係有各種的態樣，但做為其1例有例如下所稱共同論點暗號化方式之方式。

共同論點暗號化方式，係將使用於資料之暗號化論點之暗號化論點及使用於資料之譯碼化之譯碼化論點做為共同論點。在正位之使用者賦予使用之暗號化處理、譯碼化之共同論點。由於未持有之不正當使用者以暗號化資料存取，在該方式之代表性的方式有DES(資料暗號化標準：Data Encryption Standard)。

被使用於上述之暗號化處理、譯碼化之暗號化論點、譯碼化論點，係譬如根據其通行字適用雜亂信號(hash)函數等之一方向性函數可取得。所謂一方向性函數，係指由其輸出求出相反輸入係形成非常困難之函數。譬如將使用者設定之通行字做為輸入適用一方向性函數，根據其輸出以生成暗號化論點、譯碼化論點。以如此由該取得之暗號化論點、譯碼化論點，相互求出其原本之資料的通行字係實際上不可能。

又，在進行暗號化時藉由使用之暗號化論點之處理，及在進行譯碼化時使用之譯碼化論點的處理使用共同譯碼化方式被稱用所謂共同論點暗號化方式之方式。共同論點暗號化方式，係使不特定之使用者使用共同論點之論點，對於特定人暗號化文書，使該特定人使用該通行字之共同論點進行暗號化處理，藉由共同論點暗號化之文書，係對於該被使用在暗號化處理之共同論點係藉由影

五、發明說明(5)

畫形成可譯碼處理、暗號化論點，係係從發行公論點之個人所有，用以前由其公論點暗號化之文書係係保持有暗號化論點個人可進行譯碼。公論點暗號化方式之代表性方式係有RSA(Rivest-Shamir-Adleman)暗號化。

藉由利用如此之暗號化方式，將暗號化存儲信息係對正使用之者形成可譯碼之系統，對於採用此等之暗號化方式之資訊技術的存儲信息處理系統使用圖1圖解說明。

圖1係顯示PC(個人電腦)、數據庫等之再生裝置10中，由DVD、CD30、廣播網路40等之資料提供裝置用以再生取得之程式、聲音資料、影像資料等(存儲信息(Content))，同時由DVD、CD30、廣播網路40等將取得之資料做為可記憶於磁盤、記憶卡、磁帶等之記憶裝置20的構成例。

程式、聲音資料、影像資料等之存儲信息，係係形成暗號化處理，並提供於具有再生裝置10之使用者。正規使用者，係用以取得暗號化處理，同時將暗號化、譯碼化論點之論點資料。

再生裝置10係具有CPU12，將輸入資料之再生處理在再生處理部14進行執行。再生處理部14，係用以執行暗號化資料之譯碼處理，進行提供之程式的再生、聲音資料、影像資料等存儲信息再生。

正規使用者，係係提供之處理，為了再生使用在記憶裝置20進行形式/資料等，存儲信息之保存處理。在

五、發明說明(6)

再生裝置10，係為了用以執行存取存儲信息存儲處理具有存儲處理部13。存儲處理部13，係為了用以防止被記憶於記憶裝置20之資料的不正當使用。在資料利用暗號化處理用以執行保存處理。

將存儲信息進行暗號化時，係使用存儲信息暗號化論點。存儲處理部13，係使用存儲信息暗號化論點，將存儲信息進行暗號化，並將此記憶於PD(軟盤)、記憶卡、磁帶等之記憶裝置20之記憶部21。

使用者，係由記憶裝置20用以取出存儲存儲信息並進行再生時，係由記憶裝置20，用以取出暗號化資料。該在再生裝置之再生處理部14，使用存儲信息暗號化論點，即使用譯碼化論點用以執行譯碼處理並由暗號化資料用以取得譯碼資料並進行再生。

若依據圖1所示先前之構成例，則以軟盤、記憶卡等之記憶裝置20因為未將存儲存儲信息暗號化，所以由外部形成可防止不正當讀出。可是，該軟盤除其他PC、遊戲機等之資訊機器之外再被進行再生或加以利用，則相同存儲信息論點，即為了譯碼暗號化之存儲信息具有相同譯碼化論點正被再生處理則形成不可再生。因此，該軟盤之資訊機器中為了用以實現可利用之形態，將提供於使用者之暗號化論點有必要進行共同化。

可是，將存儲信息之暗號化處理進行共同化，並未持有正規暗號化之使用者暗號化處理用之論點無暗號化使用生成之可能性形成而，由於未持有正規暗號化之使用者暗號化使用

五、發明說明(7)

防止存儲信息之不正當使用的缺點，以未持有正規暗號化PC，交還該暗號等使用排除不正當使用形成困難。

又，將存儲信息之暗號化論點，該暗號化處理共同化，係由一由之機器使其暗號化資訊同一化時，便使及被該範圍會形成使用暗號化之系統全體。

進而，如上述暗號化處理共同化之環境中，係譬如在系PC上被使用，而係保存於記憶卡、軟盤等之記憶裝置之暗號化之存儲信息，係在另外之軟體可容易複製，並非原本之存儲信息資料形成可被複製狀態之利用形態。在該狀態，PC等之資訊機器中便可利用之存儲信息資料被多數複製，或會有複製之可能性。

【發明所欲解決之問題】

存儲信息資料之不正當使用，即為了用以執行未將該資料暗號化用之核對值合於存儲信息資料，即係再生過程中，根據該核對值之資料將被合於生成之核對值及存儲信息資料的核對值藉由核對處理，便進行資料驗證之方法由先前被進行。

可是，對資料在存儲信息之核對值，係對資料全體生成成為一般性，對資料全體為了用以執行被生成之核對值的核對處理，對成為核對值之資料全體生成必要用以執行核對值生成處理。譬如DES-CBC模式中藉由被生成之信息延遲生成(MAC)，進行求出核對值ICV方法時，對資料全體生成必要用以執行DES-CBC處理。該計

五、發明說明 (8)

算量，係隨著資料長與長形成進行增大，在處理效率之點有問題。

本發明，係用以解決如此習知技術之問題點，第1日的係用以提供資料處理裝置，資料處理方法及資料儲存裝置方法，以及程式提供媒體，有效用以執行資料正確性之確認處理，存儲信息資料之檢點處理的效率化，進而對檢點之記錄裝置的下載處理，就可有效用以執行檢點後之再生處理等。

又，用存儲信息資料之利用限定於正確的使用者之方法係有資料暗號化，資料隱碼化，資料驗證，認證處理，署名處理等，各種之暗號處理，為了用以執行此等各種之暗號處理，係2個之裝置間，即，用以轉送存儲信息資料之裝置間，或用以執行認證處理之裝置間，進行共有之保密資訊，單獨用以共有適用於存儲信息資料之暗號化，而暗號化的暗號資訊，或進行認證之裝置間用以共有使用於認證的暗號資訊成為必要。

因此譬如，由2個裝置的其中之一，使其具有秘密資訊的暗號資料進行密碼時，使用其共有暗號資訊之存儲信息的暗號化資料，係即使用由未持有執照之第三者也成為可譯碼，會形成不正當的存儲信息之利用。又，透過認證暗號之情形也同樣，對完全未持有執照之裝置會使認證成立，與之結果，係帶來破壞系統安全性的結果。

本發明，係用以解決如此問題點，本發明第2目的係用以提供資料處理裝置，資料處理系統，及資料處理方法

五、發明說明 (9)

而

本發明之資料處理裝置，資料處理系統，及資料處理方法，係為了資料暗號化，資料隱碼化，資料驗證，認證處理，署名處理等之暗號處理形成必要的暗號資訊不必記憶存於記憶部，而為了用以生成此等之暗號資訊將主暗號部包含於記憶部，並使暗號處理部根據主暗號，及裝置或資料之識別資料所利用生成必要的暗號資訊，從而暗號處理中之安全。

又，存儲信息資料，係根據暗號部進行提供，用以保持某程度之安全，但使被暗號於記憶部之各種的暗號資訊藉由記憶部之不正當的複製而先被取得，使暗號資訊等逃出，在未正當的執照之記錄再生器複製時，藉由複製之暗號資訊誤用不正當的存儲信息利用被形成可能。

本發明第3目的，係用以提供資料處理裝置，資料處理方法及存儲信息資料之生成方法，係為可排除此不正當的再生繼續之構成，即用以區別不正當的再生繼續，在該區別之不正當繼續中，並為構成不執行存儲信息資料之再生，下載等之處理。

又，將存儲信息資料之利用係限定於正確的使用者之方法係使用固定之暗號化暗號之暗號處理，譬如署名暗號，但選擇先前之署名之暗號處理，係使署名暗號利用存儲信息在系統之實體全體中形成為一般性的，以如此之署名暗號，係以不同的裝置形式可利用共有之存儲信息，會有發生存儲信息之不正當複製等的問題。

五、發明說明 (10)

使用資訊之進行字等用以暗號化存儲信息也可進行暗號，但進行字也可被盜用，又，透過不同的再生器經由用以輸入同一之進行字，可用以譯碼而使暗號化存儲信息資料，在先前之安全構成中，係用以限制再生器，係在其再生器用以實現利用系統係有所限制。

本發明第4目的，係提供資料處理裝置及資料處理方法，用以解決如此之先前技術的問題點，本發明之構成中，係藉由以選擇性利用資料處理裝置固有之裝置固有暗號，及利用存儲信息資料之共同於其他資料處理裝置之系統共同暗號，根據存儲信息之限制利用，係在特定之資料處理裝置中可最適用以再生存儲信息。

又，存儲信息資料，係有聲音資料，影像資料，程式資料等各種之種類，又，有必要用以暗號化存儲信息資料之全部，或使必要暗號化處理之部分及不必要暗號化處理之部分進行暗號之處理等，使各個之存儲信息存在。

如此，對各種存儲信息，一併暗號化處理進行適用，係在其再生處理中使產生不必要的暗號處理，或在處理效率，處理速度之點會產生非暗號化處理的情形，譬如像音樂資料使實際再生形成必須在資料等係為處理速度可快速譯碼處理之存儲信息資料構成為必要。

本發明第5目的，係提供資料處理裝置，存儲信息資料之生成方法，及資料處理方法，用以解決如此之問題點，本發明之資料處理裝置，存儲信息資料之生成方法及資料處理方法，係根據存儲信息資料之種類之各種存儲信息資料

五、發明說明 (11)

構成，即將根據存儲信息之不同種類的資料形式做為可適用於存儲信息，使安全性能提高且在再生，執行等中做為可容易利用存儲信息資料之生成及處理。

又，被選擇之聲音資料，影像資料等，係被輸出到A/V輸出部並被再生，可是，最近許多存儲信息係被形成為廣播型或網路型記錄媒體，或數位訊碼等，因此在再生處理之前，將此等之廣播資料形式必須加以廣播處理，譬如聲音資料則被形成MP3壓縮，則藉由MP3譯碼器被形成聲音資料之譯碼處理而被輸出，又，使存儲信息資料係音樂資料，若有MPEG2壓縮媒體，則藉由MPEG2譯碼器被形成廣播型被輸出，形成被輸出。

可是，在壓縮處理，解壓縮處理等，係有各種之種類，由存儲信息提供者透過媒體，網路等也被提供廣播資料，對於再生裝置內無此處理執行程式時，則會產生此不能進行再生之事實。

本發明第6目的，係用以提供資料處理裝置，資料處理方法及存儲信息資料之生成方法，有效用以執行廣播資料之再生處理的構成，即，有效用以執行被廣播存儲信息之聲音資料，或影像資料等情形之再生處理。

【解決問題之手段】

本發明之第1側面，

係一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的處理，其特徵在於具有：

AT

BT

五、發明說明 (13)

編號處理部，對前述存儲信息資料用以執行編號處理，及

控制部，對前述編號處理部用以執行控制；

而前述編號處理部，其構成係具有：

將存儲信息資料構成部分生成複數部分之部分資料對合 1 以上部分資料對合為複數核對值並用以生成部分核對值，藉由前述生成之部分核對值之核對處理用以執行而前述部分資料之驗證處理；同時

至少將前述部分核對值根據合 1 以上部分核對值集合資料列用以生成中間核對值，並使用該生成之中間核對值，對應於用以構成前述部分核對值集合之複數之部分核對值對該部分資料集合全體用以執行驗證處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述部分核對值，係將形成核對對象之部分資料做為為信息，藉由用以適用部分核對值生成該部分之編號處理生成之值，而前述中間核對值，係將形成核對對象之部分核對值集合資料列做為為信息，藉由適用該核對值生成該部分之編號處理生成之值，而前述編號處理部，其構成係具有用以對前述部分核對值生成該部分核對值及前述核對值生成該部分核對值。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述編號處理部，係具有複數處理部之部分核對值生成或對應於生成之部分核對值。

進而，本發明之資料處理裝置之一實施態樣中，其特

本申請案係根據中華民國專利法第 41 條第 1 項規定，將本發明之技術內容，以中文說明書、圖式及摘要，向本局提出申請。

AT

BT

五、發明說明 (13)

徵為：前述編號處理部 D E S 編號處理，而前述編號處理部，係具有可執行 D E S 編號處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述部分核對值，係將形成核對對象之部分資料做為為信息在 D E S - C B C 模式中生成之信息即生成核對值 (M A C)，而前述中間核對值，係將形成核對對象之部分核對值集合資料列做為為信息在 D E S - C B C 模式中生成之信息即生成核對值 (M A C)，而前述編號處理部，係具有藉由 D E S - C B C 模式用以執行編號處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：藉由具有前述編號處理部之 D E S - C B C 模式之編號處理構成，係在形成核對對象之信息即之一部分被處理三倍之 D E S 之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係具有等名輪匙，而前述編號處理部，係對前述中間核對值藉由適用前述等名輪匙將該生成之值為了資料驗證處理而進行驗證之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係作為等名輪匙具有複數之等名輪匙，而前述編號處理部，係具有根據前述存儲信息資料之限制利用等名輪匙之等名輪匙而前述等名輪匙對前述中間核對值進行驗證於編號處理為資料驗證值與核對值之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特

本申請案係根據中華民國專利法第 41 條第 1 項規定，將本發明之技術內容，以中文說明書、圖式及摘要，向本局提出申請。

AT

BT

五、發明說明 (14)

徵為：前述資料處理裝置，係為前述該複數之等名輪匙，具有用以執行資料驗證處理共同於系統之全體資料之共同等名輪匙，及用以執行資料驗證處理之各部分之裝置固有之裝置固有等名輪匙。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述部分核對值，係合：其部分核對值，對於用以構成資料之一部分之無管理內資料被生成以上；及存儲信息核對值，對於用以構成資料之一部分之存儲信息即部分資料被生成以上；而前述編號處理部，其構成係具有對前述無管理內資料之部分資料集合用以生成 1 以上之無管理內核對值並用以執行核對處理，而對於前述存儲信息即部分資料之部分資料集合用以生成 1 以上之存儲信息核對值並用以執行核對處理，進而，根據生成之前述無管理部分核對值及前述存儲信息核對值全部用以生成該核對值並藉由用以執行核對處理用以執行資料驗證。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述部分核對值，係合無管理部分核對值，對於用以構成資料之一部分之無管理內資料被生成以上；而前述編號處理部，其構成係具有對前述無管理內資料之部分資料集合用以生成 1 以上之無管理部分核對值並用以執行核對處理，進而，用以構成生成之前述 1 以上之無管理部分核對值及前述資料之一部分之存儲信息即部分資料所構成資料列用以生成核對值並藉由用以執行核對處理用以執行資料驗證。

本申請案係根據中華民國專利法第 41 條第 1 項規定，將本發明之技術內容，以中文說明書、圖式及摘要，向本局提出申請。

AT

BT

五、發明說明 (15)

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係為前述其特徵為：在前述編號處理部中具有記錄裝置用以記錄正當性驗證之核對值之資料。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置中，部分核對值之核對處理中，並未生成核對值，其特徵為：前述控制部，係對前述記錄裝置具有用以中止該核對處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係在前述編號處理部中，部分核對值之核對處理中，在生成核對值之前，其特徵為：前述控制部，係在生成核對值之前，其特徵為：在前述編號處理部中具有中止該核對處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係在前述編號處理部中，部分核對值之核對處理中，在生成核對值之前，其特徵為：在前述編號處理部中具有中止該核對處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係在前述編號處理部中，部分核對值之核對處理中，其特徵為：具有控制裝置用以執行資料之無管理部分核對值的核對處理，並將成立無管理部分核對值之核對的資料轉送於前述再生處理部並作為再生等。

進而，本發明之第二方面。

係一資料驗證裝置，藉由記憶裝置或通訊機構進行該提供之存儲信息資料的處理，其特徵在於具有：

編號處理部，對前述存儲信息資料用以執行編號處理，及

本申請案係根據中華民國專利法第 41 條第 1 項規定，將本發明之技術內容，以中文說明書、圖式及摘要，向本局提出申請。

A7

B7

五、發明說明 (15)

際制部，對前述暗號處理部用以執行控制；

而前述暗號處理部，其構成係具有：

驗證對象資料係暗號化資料時，藉由該暗號化資料之譯碼處理部取得譯碼資料用以執行譯碼處理部取得暗號資料處理結果資料藉由用以實施通用者名稱之暗號處理，用以生成驗證對象資料之驗證值。

進而，本發明之資料處理裝置之一實施態樣中，前述暗號處理，其特徵為：藉由前述暗號化資料之譯碼處理部取得譯碼資料以與通用者名稱進行譯碼處理與演算之處理。

進而，本發明之第3側面，

係一種資料處理方法，藉由此種譯碼處理部取得進行被提供之存儲信息資料的處理，其特徵在於：

將存儲信息資料構成部分或構成部分之部分資料對合1以上部分資料集合後為該部分並用以生成部分驗證值，藉由用以供該生成部分或驗證值之處理用以執行前述部分資料之驗證處理；

而前述部分驗證值係對合1以上部分資料對合後資料利用以生成中間驗證值，並使用該生成中間驗證值對照於用以構成前述部分驗證值之複數的部分驗證值對照表之部分資料集合全數用以執行驗證處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述部分驗證值，係將前述驗證對象之部分資料做為信息，具有藉由用以適用部分驗證值生成驗證值之暗號

本申請案係依據中華民國專利法第101條第1項第1款規定提出

本申請案係依據中華民國專利法第101條第1項第1款規定提出

- 10 -

A7

B7

五、發明說明 (17)

處理部生成之值，而前述中間驗證值，係將前述驗證對象之部分驗證值集合資料列做為信息，具有藉由用以適用暗號處理生成驗證值之暗號處理部生成之值。

進而，本發明之資料處理方法之一實施態樣中，前述部分驗證值，其特徵為：對應於該生成之部分驗證值用以適用不同種類之部分驗證值生成暗號並進行生成者。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述暗號處理係D E S暗號處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：

將前述部分驗證值，係將前述驗證對象之部分資料做為信息並在D E S-C B C模式中生成之信息並行將該(M A C)，而前述中間驗證值，係將前述驗證對象之部分驗證值集合資料列做為信息並在D E S-C B C模式中生成之信息並行將該(M A C)。

進而，本發明之資料處理方法之一實施態樣中，進而其特徵為：前述中間驗證值係藉由通用者名稱之暗號處理部生成之值為資料驗證值為驗證值並加以應用者。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：根據資料利用選擇不同者名稱暗號對照表中間驗證值用以暗號處理為資料驗證值為驗證值。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：根據前述者名稱，係將用以執行資料驗證處理共同於系統之全實體的共同者名稱，及用以執行資料驗證

本申請案係依據中華民國專利法第101條第1項第1款規定提出

本申請案係依據中華民國專利法第101條第1項第1款規定提出

本申請案係依據中華民國專利法第101條第1項第1款規定提出

- 20 -

A7

B7

五、發明說明 (15)

處理之各個驗證值有以驗證值有者名稱暗號處理資料之限制利用標準進行選擇並加以應用。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：

前述部分驗證值，係合：管理部分驗證值，對於用以構成資料之一部分之管理部分資料生成1以上；及存儲信息驗證值，對於用以構成資料之一部分的存儲信息部分資料生成1以上；而前述資料驗證處理，係對於前述管理部分資料之一部分資料集合用以生成1以上之管理部分驗證值並用以執行驗證處理，而對於前述存儲信息部分資料之一部分資料集合用以生成1以上之存儲信息驗證值並用以執行驗證處理，進而，前述生成之前述管理部分驗證值及前述存儲信息驗證值全部用以生成驗證值並用以執行資料驗證。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：

前述部分驗證值，係合管理部分驗證值，對於用以構成資料之一部分之管理部分資料生成1以上，而前述資料驗證處理，係對於前述管理部分資料之一部分資料集合用以生成1以上之管理部分驗證值並用以執行驗證處理，進而，用以構成生成之驗證值1以上的管理部分驗證值及前述資料之一部分根據存儲信息部分資料所生成資料利用以生成驗證值並藉由用以執行驗證處理用以執行資料驗證。

本申請案係依據中華民國專利法第101條第1項第1款規定提出

本申請案係依據中華民國專利法第101條第1項第1款規定提出

- 21 -

A7

B7

五、發明說明 (15)

進而，本發明之資料處理方法之一實施態樣中，其特徵為：資料之驗證值，進而將驗證完成資料處理進行存於記錄裝置。

進而，本發明之資料處理方法之一實施態樣中，前述部分驗證值之驗證處理中，使該對未能成立之情形中，其特徵為：用以中止存儲處理進而將該記錄裝置並用以執行控制。

進而，本發明之資料處理方法之一實施態樣中，前述部分驗證值之驗證處理中，使該對未能成立之情形中，其特徵為：在該處再生處理部用以中止再生處理並用以執行控制。

進而，本發明之資料處理方法之一實施態樣中，前述部分驗證值之驗證處理中，其特徵為：將用以執行資料之管理部分驗證值的驗證處理，將成立管理部分驗證值之驗證的資料轉送到前述再生處理部做為可再生並用以執行控制。

進而，本發明之第4側面，

係一種資料處理方法藉由記錄裝置或通訊裝置進行所提供之存儲信息資料之處理，其特徵在於：

驗證對象資料係暗號化資料時，藉由該暗號化資料之譯碼處理部取得譯碼資料用以執行譯碼處理。

藉由前述暗號處理部取得之譯碼處理結果藉由用以執行適用者名稱之暗號處理用以生成前述驗證對象資料之驗證值。

本申請案係依據中華民國專利法第101條第1項第1款規定提出

本申請案係依據中華民國專利法第101條第1項第1款規定提出

本申請案係依據中華民國專利法第101條第1項第1款規定提出

- 22 -

A7
B7

五、發明說明(20)

進而，本發明之資料驗證賦予方法之一實施態樣中，其特徵為：前述驗證處理，係藉由前述暗號化資料之譯碼處理將被取得之譯碼資料以預定單元位進行排他性邏輯和演算之處理。

進而，本發明之第5方面，

係一種資料驗證賦予方法，為資料驗證處理之資料驗證賦予方法

將資料分派成複數部分之部分資料合1以上對部分資料集合成為核對值賦予部分核對值。

至少將前述部分核對值合1以上對部分核對值集合資料列進行驗證其中間核對值賦予驗證對象資料。

進而，本發明之資料驗證賦予方法之一實施態樣中，其特徵為：前述部分核對值，係形成核對對象之部分資料做為信息，藉由用以適用部分核對值生成輸出之暗號處理後生成之值，而前述中間核對值，係將形成核對對象之部分核對值集合資料列做為信息，藉由適用總核對值生成之暗號處理後生成之值。

進而，本發明之資料驗證賦予方法之一實施態樣中，其特徵為：前述部分核對值，係對應於生成之部分核對值用以適用不同種類之部分核對值生成輸出並進行生成。

進而，本發明之資料驗證賦予方法之一實施態樣中，其特徵為：前述暗號處理係DES 5暗號處理。

進而，本發明之資料驗證賦予方法之一實施態樣中，其特徵為：前述部分核對值，係將形成核對對象之部分

本國代理人通商中國商務事務所 (CNS) JA 成員 (210+207 公室) - 23 -

A7
B7

五、發明說明(21)

資料做為信息在 DES-CBC 模式中生成之信息驗證符號 (MAC)，而前述中間核對值，係將形成核對對象之部分核對值集合資料列做為信息在 DES-CBC 模式中生成之信息驗證符號 (MAC)。

進而，本發明之資料驗證賦予方法之一實施態樣中，其特徵為：對前述中間核對值係藉由適用署名輸出之暗號處理後生成之值為資料驗證做為核對值並加以適用者。

進而，本發明之資料驗證賦予方法之一實施態樣中，其特徵為：前述資料之限制利用驗證將不同署名輸出對照集中間核對值適用於暗號處理為資料驗證做為核對值。

進而，本發明之資料驗證賦予方法之一實施態樣中，其特徵為：做為前述署名輸出，係利用以執行資料驗證處理共同於系統之全實體的共同署名輸出，以及以執行資料驗證處理之各種裝置間有署名輸出根據資料之限制利用增加以適用處理是增加以使用者。

進而，本發明之資料驗證賦予方法之一實施態樣中，其特徵為：前述部分核對值，係合1、憑著部分核對值，對用以構成資料之一部分之憑著部分內資料被生成1以上；及存儲信息核對值，對用以構成資料之一部分的存儲信息部內資料被生成1以上；並對前述憑著部分核對值及前述存儲信息核對值全部用以生成核對值並進行發送能用以執行資料驗證者。

本國代理人通商中國商務事務所 (CNS) JA 成員 (210+207 公室) - 24 -

A7
B7

五、發明說明(22)

進而，本發明之資料驗證賦予方法之一實施態樣中，其特徵為：前述部分核對值，係合1、憑著部分核對值對用以構成資料之一部分之憑著部分內資料被生成1以上，用以構成前述1以上之憑著部分核對值及前述資料之一部分對由存儲信息同步資料所構成資料列全部用以生成核對值並進行發送能用以執行資料驗證。

進而，本發明之第6方面，

係一種程式供應裝置，用以提供電腦程式執行資料正實性之驗證的資料驗證處理在電腦系統上執行，其特徵在於：

前述電腦程式供應：

將資料分派成複數部分之部分資料合1以上之部分資料集合成為核對值並藉由被生成之部分核對值的核對處理用以執行前述部分資料之驗證處理的步驟；及

使前述部分核對值根據複數組合之部分核對值集合使用被生成之中間核對值，用以構成前述部分核對值集合對應於複數的部分核對值對應於複數之部分資料集合全體用以執行驗證處理的步驟。

進而，本發明之第7方面，

係一種資料處理裝置，其特徵為：

具有：暗號處理部，用以執行資料暗號化，資料譯碼化，資料驗證，認證處理，署名處理之至少其中一種的暗號處理；

認證部，用以容納主鑰匙為用以生成適用於認證暗

本國代理人通商中國商務事務所 (CNS) JA 成員 (210+207 公室) - 25 -

A7
B7

五、發明說明(23)

號處理的輸出：

而前述暗號處理部，其構成係具有將用以執行前述暗號處理必要的個別輸出，根據前述主鑰匙，及暗號處理對象之信息或資料之識別資料進行生成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係透過記憶部或通訊部進行關於轉送資料之暗號處理的資料處理裝置，而前述記憶部，係具有用以生成適用於前述轉送資料之暗號處理的記憶輸出 Kdis 並用以容納記憶輸出生成用主鑰匙 Mdis，而前述暗號處理部，係根據被容納於前述記憶部之記憶輸出生成用主鑰匙 Mdis，及前述暗號資料之識別資料的資料識別子用以執行暗號處理，並用以生成前述轉送資料之記憶輸出 Kdis 的構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係形成轉送資料之轉送對象或前述進行外信連接裝置之認證處理的資料處理裝置，而前述記憶部，係具有用以生成前送外信連接裝置之認證輸出 Kake 並用以容納認證輸出生成用主鑰匙 Make，而前述暗號處理部，係根據被容納於前述記憶部之認證輸出生成用主鑰匙 Make，及前述外信連接裝置之識別資料的外信連接裝置識別子用以執行暗號處理，並用以生成前述外信連接裝置之認證輸出 Kake 的構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係對資料用以執行暗號處理的

本國代理人通商中國商務事務所 (CNS) JA 成員 (210+207 公室) - 26 -

五、發明說明 (25)

轉送資料之轉送對象或轉送途徑的外部運送裝置之認證處理，而前述論點生成步驟，係根據用以生成前述外部運送裝置之認證論點 Kake 之認證論點生成用主論點 Mlike，及前述外部運送裝置之識別資訊之外部運送裝置識別子用以執行暗號處理，並用以生成前述外部運送裝置之認證論點 Kake 之認證論點生成步驟，而前述暗號處理步驟，係根據前述認證論點生成步驟中執行生成之認證論點 Kake 用以執行外部運送裝置之認證處理的步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：

前述資料處理方法中之進行執行的資料處理，係對資料之署名處理，而前述論點生成步驟，係根據用以生成前述資料處理裝置之資料處理裝置署名論點 Kdev 的署名論點生成用主論點 Mlikev，及前述資料處理裝置之識別資料的資料處理裝置識別子用以執行暗號處理，並用以生成前述資料處理裝置之資料處理裝置署名論點 Kdev 的署名論點生成步驟，而前述暗號處理步驟，係根據前述署名論點生成步驟中執行生成之署名論點 Kdev 用以執行資料之署名處理的步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述論點生成步驟，係將暗號處理對象之假設或資料之識別資料至少一部分作為信息，並同時將主論點做為暗號論點進行適用之暗號處理。

進而，本發明之資料處理方法之一實施態樣中，其特

本國際技術性文件係根據 PCT/JP98/0054 號專利申請案之說明書及圖式所編譯而成。

五、發明說明 (25)

徵為：前述暗號處理係適用 D R S 算法之暗號處理。

進而，本發明之第 10 個實例，

係一種資料處理方法，由提供存儲信息資料之存儲信息資料提供裝置，及進行存儲信息資料之利用的存儲信息資料利用裝置所構成資料處理系統中之資料處理方法，其特徵在於：

前述存儲信息資料提供裝置，係根據用以生成適用於存儲信息資料之暗號處理的存儲信息資料配送論點之配送論點生成用主論點，及提供存儲信息資料之識別子之存儲信息識別子用以生成存儲信息資料配送論點，並用以執行該存儲信息資料之暗號處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：

前述存儲信息資料提供裝置，係具有複數不同之配送論點生成用主論點為用以生成複數不同之存儲信息資料配送論點，並根據該複數之配送論點生成用主論點及前述存儲信息識別子以生成複數不同之存儲信息資料配送論點，經由該生成之複數的配送論點用以執行暗號處理並用以生成複數不同之暗號化存儲信息資料，而前述存儲信息資料利用裝置，係具有前述存儲信息資料提供裝置有的複數不同之配送論點生成用主論點之至少 1 個之配送論點生成用主論點，使用自己所有之配送論點生成用主論點及前述配送論點生成用主論點經由生成之配送論點配送將暗號化存儲信息資料進行譯碼。

本國際技術性文件係根據 PCT/JP98/0054 號專利申請案之說明書及圖式所編譯而成。

五、發明說明 (33)

進而，本發明之第 11 個實例，

係一種資料處理方法，藉由假設之資料處理裝置被構成資料處理系統中之資料處理方法，其特徵在於具有：

在前述假設之資料處理裝置中之 1 個資料處理裝置 A 中，根據存儲信息資料生成用主論點為用以生成適用於存儲信息資料之暗號處理的存儲信息論點，及該資料處理裝置 A 之裝置識別子經由該生成之存儲信息論點暗號處理之存儲信息資料資料於記憶媒體之步驟，在另一資料處理裝置 B 中，根據前述資料處理裝置 A 及同一之前述存儲信息論點生成用主論點及前述資料處理裝置 A 之裝置識別子用以生成前述存儲信息論點及同一存儲信息論點之步驟，及在另一資料處理裝置 B 經由生成之存儲信息論點進行非於前述記憶媒體之存儲信息資料之譯碼的步驟。

進而，本發明之第 12 個實例，

係一種資料處理方法，由主裝置，及形成該主裝置之認證處理對象的副裝置所構成之資料處理系統中之資料處理方法，

前述副裝置，係根據認證論點生成用主論點為用以生成適用於主裝置及副裝置間之認證處理的認證點，及該副裝置之識別子之副裝置識別子用以生成認證論點，並對生成之認證論點進行於該副裝置內之記憶處理，

而前述主裝置，係根據前述認證論點生成用主論點，及前述副裝置之識別子之副裝置識別子用以生成認證論點並用以執行認證處理。

本國際技術性文件係根據 PCT/JP98/0054 號專利申請案之說明書及圖式所編譯而成。

五、發明說明 (33)

進而，本發明之第 13 個實例，

係一種程式提供裝置，用以提供程式裝置並用以執行資料暗號化，資料譯碼化，資料驗證，照像處理，署名處理至少其中之一之暗號處理並同時將暗號處理在電腦系統上執行之程式提供裝置，其特徵在於：

前述暗號化程式，係含有：

將執行暗號處理必要之識別論點，根據主論點為用以生成適用於前述暗號處理之論點，及暗號處理對象之裝置或資料之識別資料進行生成之論點生成步驟；及

藉由前述論點生成步驟將暗號處理之論點並用以執行暗號處理的暗號處理步驟。

本發明之第 14 個實例，

一種資料處理裝置，係藉由記憶媒體或通訊網路進行提供存儲信息資料之處理的資料處理裝置，其特徵在於具有：

記憶部，用以容納資料處理裝置識別子；

名驗證部，用以抽出包含於存儲信息資料中之不正當簽名名單，並用以執行該名單內之參加者及被參加者於前述記憶部之前述資料處理裝置識別子的核對處理；及

核對部，前述核對處理中之核對處理結果，包含有在前述不正當簽名名單中與前述資料處理裝置識別子一致的資訊時，用以中止對前述存儲信息資料之再生或記憶裝置的資料處理至少其中之一之處理執行。

進而，本發明之資料處理裝置之一實施態樣中，其特

本國際技術性文件係根據 PCT/JP98/0054 號專利申請案之說明書及圖式所編譯而成。

五、發明說明 (32)

查為：前述名單經證部，係具有暗號處理部用以執行前述存儲信息資料的既設處理，而前述暗號處理部，係根據符合於前述存儲信息資料不正當機器名單之核對使用以驗證有無前述不正當機器名單的篡改，並藉由該驗證，僅判定形成篡改時用以執行前述核對處理之構成。

然而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，具有不正當標榜名單核對生成模組，而將前述暗號處理部，係對前述生成之不正當標榜名單構成資料以執行適用前開不正當標榜名單核對生成模組的暗號處理並用以生成不正當標榜名單核對值，並用以執行該值生成之不正當標榜名單核對值，及被食飲部或該值生成資料中不正當標榜名單之核對值核對並用以確定有無前述不正當標榜名單之篡改的構成。

通而，本發明之資料處理裝置之一實施態樣中，其特徵在於：前述名單驗證部，係具有確號處理部用以執行對該存儲假信息資料之編號處理，再將該確號處理部，係用以執行被舍於前述存儲假信息資料中依確號化之不正當獲悉者名單的篩選處理，做為該篩選處理之結果對於被取得之不正當獲悉名單用以執行刪除該處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述名單驗證部，係藉由串接處理部用以執行與形成存儲信息資料之轉送對象或轉送源之記憶裝置的相互認證處理，而前述名單驗證部，係藉由前述串接處理部與前述被執行前述記憶裝置之相互認證處理部成立認證做為條件。

經濟學原理及應用二講堂作版權

五、發明說明 (33)

件，用以抽出被含於前述存儲信息資料中不正當機器名單與被容納於前述記憶部之前述資料處理裝置識別子用以執行檢製處理之構成。

進而，本發明之第 15 側面，

係一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理方法，其特徵係具有：

用以抽出並含於存儲信息資料中不正當機關名單之名稱抽出步驟：

藉由前述名單抽出步驟被含於被抽出之名單的參加者，及被容納於資料處理裝置內之記憶部的前述資料處理裝置區別子用以執行核對處理之核對處理步驟；及

前述類對處理步驟中之核對處理結果，在前述不正當機關名單中含有與前述資料處理類別予一致的資訊時，用以中止前述存儲信息資料之再生或對記錄裝置之容納處理至少其中之一之處理執行之步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係進而，合類被包含於前述非創信息資料中不正當機器名單之核對僅用以驗證有無前述不正當機器名單之竄改的驗證步驟，而前述核對處理步驟，係藉由前述驗證步驟，獲進行判定形成竄改跡進行執行。

範圍，本章開之資料處理方法之一實施結構中，其步

經濟學原理與應用 王清惠主編

五、發明說明 (34)

構成資料用以執行適用不正當機密名單核對值生成鏈匙之除錯處理並用以生成不正當機密名單核對值的步驟，及用以執行生成之不正當機密名單核對值，及被含於前述存儲信息資料中不正當機密名單核對值的核對並用以驗證有無前述不正當機密名單之更改的步驟。

是謂，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係選擇，當用以執行包含於該存取個位電資料庫中該標誌化之不正當機器名單的譯碼處理之譯碼步驟，而前述該對處理步驟，係做為前述譯碼步驟之結果對於被取尋之不正當機器名單用以執行前述該對處理

進而，本發明之資料處理方法之一實施型態中，其特徵為：前述資料處理方法，係透過，含形成存儲信息資料之轉送對需求轉送率與記錄表資訊互認部處理步驟，而藉此部處理結果，係藉由前述相互認部處理步驟與該執行造紀錄表資訊根據相互認部處理兩部進行成立認部做為條件用以執行前述控制處理。

進而，本發明之第 16 個置，

係一種存儲信息資料生成方法，藉由記憶媒體或通訊媒體對複數之記錄再生器進行被提供存儲信息資料之生成之存儲信息資料生成方法，其特徵為：

惟為存儲信息資料之集管資訊形成該存儲信息資料之利用排除對象時記錄再生器之記錄再生器識別子用以容納做為構成資料之不正當標語名單並做為存儲信息資料。

經濟部智慧財產局及農工部農會等亦在內。

五、林曜如題 / 35

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵為：檢尋存儲信息資料之集管資訊，用以容納前述不正當搜尋名單之資訊該對用的不正當機器名單相對組者。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵為：將該遮罩電機名單進行暗號化並密納於存儲信息資料之加密資訊中。

進而，本發明之第 17 例置，

係一種程式提供媒體，用以提供電腦程式藉由記憶媒體或通訊媒體將被提供存儲信息資料之處運在電腦系統上執行的程式提供媒體，其特徵在於：前述電腦程式，係具有：

用以抽出被含於存儲信息資料中不正當機關名單之名單抽出步驟：

藉由前述名單抽出步驟被含於被抽出之名單的參加者，及被含納於資料處理裝置內之記憶部的前述資料處理裝置微處理器用以執行核對處理之核對處理步驟；及

前述核對處理步驟中之核對處理結果，在前述不正當機器名單中含有與前述資料處理識別子一致的資訊時，用以中止前述存儲信息資料之再生或對記錄裝置之容納處理至少其中之一的處理執行之步驟。

進而，本發明之第18例圖，係一種資料處理裝置，藉由記憶媒體或通訊媒體進行檢提供存儲信息資料之處理之資料處理裝置，其特徵在於其構成具有：

經濟部智慧財產局員工消費合作社印

五、發明說明 (36)

暗號處理部，對前述存儲信息資料用以執行暗號處理

控制部，對前述繪製處理部用以執行控制：

系統共同輸出，被使用於前述暗號處理部中之暗號處理，並共同於利用前述存儲信息資料之其他的資料處理裝置；及

裝置固有識別子至少其中之一，爲了用以生成被使用於前述暗號處理部中之暗號處理的資料處理裝置固有之裝置固有地址或該裝置固有地址；

而刺迷暗壁成理部

係根據前述存儲信息資料之利用型態將前述系統共同繪出，或前述裝置固有繪出之其中之一適用於前述存儲信息資料並用以執行編號處理。

進而，本發明之資料處理裝置之一實施型態中，其特徵為：前述編號處理部，其構成具有根據被含於前述存儲信息資料之規則利用資訊處理前述系統共同編號，或前述類型固有編號於其中之一適用於前述存儲信息資料並用以執行編號處理。

是而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係進而，具有記錄裝置用以記錄存儲信息資料，而前述讀取裝置，係將前述存儲信息資料僅放在自己之資料處理裝置並將有使用之限制利用時，對前述存儲信息資料使用前述裝置圖有鎖匙用以執行唯讀裝置並用以生成容納資料到前述記錄裝置，並將前述

五、發明說明 (37)

個信息資料放在自己之資料處理裝置以外也可做為使用時，對該處存儲信息資料使用前述系統共同輪匙用以執行增減處理並用以生成容納資料材料雜誌裝置。

進而，本研究以資料或資訊之實一實態為核心，其特點為：因該資料庫或資訊，係具有資料處理與資訊處理之專業名稱 Kdey，及在環境之資料處理與資訊處理之系統等名稱 Ksys，而該系統與資料庫，其前導這些存儲態係資訊係在各自之資料庫或資訊庫所有之限制與約束是密切的，因此記錄與資訊時，對前述存儲態係資料適用前述資料庫固有之專業名稱與由該系統應用以生成與資訊庫有以之系統，將前述存儲態係資料係在各自之資料庫或資訊庫有以之狀態也為其為可使用基於前述狀態與結果，對前述存儲態係資料適用前述系統名稱 Kdey，Ksys 輸出時該系統應用以生成與資訊庫，而前述系統，係前述這些處理態之生成之前述狀態與有統制與或前述狀態但對其之一之前述存儲態係資料一起對前述狀態與結果應用以施行統制。

進西，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，其構成係具有資料處理裝置固有之署名輪匙 *Kdev*，並在複數之資料處理裝置共同之系統署名輪匙 *Ksys*，而前述暗號處理部，係僅放在自己之資料處理裝置內以再生物理上有使用上之便利利用的存儲信息資料時，對前述存儲信息有適用前述裝置固有之署名輪匙 *Kdev* 藉由暗號處理用以生成裝置固有相對值，並用以執行該系統性之裝置固有相對值的相對處理，故在自己之資料

五、發明說明 (38)

過是裝置以外的媒體也被做為可使用以再生根附有限制利用之存儲信息資料時，對前述存儲信息資料適用前述系統管理策略 Key 藉由學號處理以生成過換對值，並用以執行該生成後之總核對值的總核處理。而前述總核部，係從前述裝置固有板對立之核對成立後之情形，或從前述總核對處理之核對成立後之情形以存儲信息資料之總核處理部便處理之總核並用以生成可再生媒體資料。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，其構成係具有記錄資料處理裝置名稱此主輪匙 Mkdex，及資料處理裝置識別子 Idex，而前述增設處理部，係根據前述資料處理裝置等名稱及主輪匙 Mkdex 及前述資料處理裝置識別子 Idex 藉由暗號直接做為資料處理裝置固有輪匙用以生成署名輪匙 Key。

進而，本發明之資料處理裝置之一實施態樣中，其特
點為：前述暗號處理部，其構成係對前述資料處理裝置與
例子 IDaaS 應用前述資料處理裝置署名鑰匙用主鑰匙藉由
DES 暗號處理用以生成前述署名鑰匙。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述暗號處理部，係對前述存儲信息資料用以執行暗號處理並用以生成中間核對值，在該中間核對值適用前或資料處理裝置固有鑰匙或系統共有鑰匙用以執行暗號處理。

五、發明說明 (39)

將成簇數部分後之部分資料對含 1 以上部分資料集合藉由暗號處理用以生成部分核對值，含生成後之部分核對值對部分核對值集合資料列藉由暗號處理用以生成中間核對值。

進而，本發明之第 19 個更，

係一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理方法，其特徵在於

根據前述存儲信息資料之利用態樣，

用以選擇利用前述存儲信息資料共通於其他資料處理裝置之暗號處理用系統共同編號。或，資料處理裝置固有之裝置固有編號與其中之一的暗號處理編號。

將選擇後之暗號處理輸出適用於前述存儲信息資料用以執行檢覽處理。

進而，本明之資料處理方法之一實施想像中，對前述資料處理方法中之存儲係指資料的歸類與登記之記錄簿面中，其特徵為：將前述存儲係指資料僅放在自己之資料處理裝置並附有使用之限制利用時，對前述存儲係指資料使用前述裝置即有權使用以執行數據處理並用以生成查詢資料以創造登記簿面，而將前述存儲係指資料也放在自己之資料處理裝置以外做為可使用時，對前述存儲係指資料使用前述系統共同權能用以執行數據處理並用以生成查詢資料以創造登記簿面。

進而，本發明之資料處理方法之一實用態樣中，對前

五、發明說明 (49)

遠資料處理方法中之存儲信息資料的記錄裝置之記錄處理中，其特徵為：將前述存儲信息資料僅放在自己之資料庫裝置供有使用之限制利用並置於前述記錄裝置時，對前述存儲信息資料適用前述裝置固有之著名編號 Kdev 後，由庫裝置應用以生成裝置固有核對值，將前述存儲信息資料也放在自己之資料處理裝置以外的裝置做為可使用並置於前述記錄裝置時，對前述存儲信息資料適用前述系統著名編號 Sysv 後由庫裝置生成用以生成核對值。

並將前述生成後之前述裝置固有核對值或前述總核對值其中之一與前述存儲信息資料一起容納於前述記錄裝置。

經濟學原理及應用二講堂筆記

五、發明說明 (45)

進而，本發明之資料處理方法之一實施態樣中，其特徵為：合併將資料處理裝置署名輪匙用主輪匙 Mkdev 及資料處理裝置識別子 IDdev 藉由唯讀裝置做為資料處理裝置固有輪匙用以生成署名輪匙 Kdev 之步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述署名公鑰匙 Kdev 生成步驟，係對前述資料處理裝置類別 IDdev 適用前述資料處理裝置署名公鑰匙用主鑰匙 Mkdev 後藉由 DES 暗號處理用以生成前述署名公鑰匙 Kdev 之步驟。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係進而，含對前述存儲信息資料用以執行增減處理並用以生成中間核對值之步驟，在前述中間核對值適用前述資料處理與覆固有關態或系統共有編號後用以執行增減處理。

通而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係透過，將前述儲存信息資料分割成複數部分後之部分資料對合 1 以上部分資料集合而由暗號處理用以生成部分核對值，對合該生成後之部分核對值的部分核對值集含資料判斷由暗號處理用以生成中間核對值。

係一種程式提供媒體，提供電腦程式藉由記憶媒體或通訊媒體進行被提供存儲信息資料之處理將資料處理在電腦系統上執行之程式媒體，其特徵在於：

100

五、聲明說明 (43)

根據前述存儲信息資料之利用態樣，

用以選擇利用前述存儲信息資料共通於其他資料處理裝置之暗號處理用系統共同鑰匙，或，資料處理裝置固有之暗號固有鑰匙其中之一的暗號處理鑰匙之步驟。

將選擇後之哈號處理辦法適用於前述存儲信息資料用以執行哈號處理之步驟。

再者，本發明之第 21 個圖，

係一種資料處理裝置，藉由記錄媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理裝置，其特徵在於其構成具有：

暗號處理部，對前述存儲信息資料用以執行暗號處理；及

控制部，對前述設備處理係用以執行控制：

西藏經濟發展研究

係在含於資料驗證對象之存儲信息區設資料單位用以生成存儲信息核對值，藉由用以執行生成該之存儲信息核對值之核對處理，用以執行前述資料中之存儲信息區設資料單位的正常性檢驗處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，其構成具有存儲信息核對發生成信息，而前述處理裝置，係根據驗證對象之存儲信息區段資料用以生成存儲信息中間值，並對該存儲信息中間值適用前述存儲信息核對發生成信息使用以執行暗號處理，並用以生成存儲信息核對值。

經濟師智德財星局員工消費合作社印製

五、發明說明 (43)

再者，本發明之資料處理裝置之一實施態樣中，其特徵為：前述驗證處理部，係使驗證對象之存儲信息區段資料被串接化時，藉由該存儲信息區段資料之譯碼處理被取得譯碼文全數以預定組元單位進行預定之演算處理並用以生成存儲信息中間率，使驗證對象之存儲信息區段資料未被串接化時，將存儲信息區段資料全數以預定組元單位進行預定之演算處理用以生成存儲信息中間率。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：在前述暗號處理部之前述中間核對僅的生成處理進行適用前述預定之演算處理係排他性邏輯和演算。

然而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述暗號處理部，係藉由 C B C 模式具有雜號處理構成，而使驗證對象之存儲信息同步資料被暗號化時適用於存儲信息中間信生成處理之前述雜碼處理，係藉由 C B C 模式之雜碼處理。

然而，本發明之資料處理裝置之一實施態樣中，其特
應為：藉由具有前述暗號處理部之 C B C 模式之暗號處理
構成，係構成僅在形成處理對象之信息列的一部分被適用
於對其基圖輪廓線處理。

進而，本發明之資料處理裝置之一實施態樣中，其暫微為：前述編號處理部，係構成在存儲信息區段資料含有複數之零件，並使被合於該存儲信息區段資料一部分之零件有驗證對象時，根據驗證對象零件用以生成存儲信息標對標，並藉由用以執行生成後之存儲信息標對標的核對。

未經修正之適用中國國家標準 GB2853-84 規格 1714 × 252 公釐

五、發明說明 (45)

理，用以執行前述資料中之各存儲信息區段資料單位的正常性驗證處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述驗證處理部，其構成係在前述存儲信息區段資料包含有複數之零件，使驗證對象之要驗證零件有1個時，使前述要驗證零件未被破壞化時，藉由要驗證零件之譯碼處理將取得譯碼文全體以預定組元單位進行逐段驗證和後之值，適用存儲信息核對值生成驗證後用以執行驗證處理並用以生成存儲信息核對值，從而前述驗證零件未被破壞化時，將該要驗證零件全體以預定組元單位進行逐段驗證和後之值，適用前述存儲信息核對值生成驗證後用以執行驗證處理並用以生成存儲信息核對值。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述驗證處理部，其構成係在前述存儲信息區段資料包含有複數之零件，使驗證對象之要驗證零件有複數時，在各零件適用存儲信息核對值生成驗證後用以執行驗證處理取得後之零件核對值的邏輯處理，進而適用前述存儲信息核對值生成驗證後用以執行驗證處理將取得結果做為存儲信息核對值。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係進而，在前述驗證處理部中具有記錄裝置用以收納存儲信息資料舍被執行正常性驗證後之存儲信息區段資料。

進而，本發明之資料處理裝置之一實施態樣中，在前

五、發明說明 (45)

述驗證處理部中之存儲信息核對值的核對處理中，在未來成立核對後之情形，其特徵為：前述控制部，其構成係具有用以中止容納處理到前述記錄裝置。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係進而，在前述驗證處理部中具有再生處理部用以再生被執行正常性驗證後之資料。

進而，本發明之資料處理裝置之一實施態樣中，前述資料處理裝置，係在前述驗證處理部中之存儲信息核對值的核對處理中，在未來成立核對後之情形，其特徵為：前述控制部，其構成係具有在前述再生處理部用以中止再生處理部。

進而，本發明之第2個側面，

係一種資料處理方法，係由記錄裝置透過通訊媒體進行被提供存儲信息資料之處理的資料處理方法。

係在含於資料驗證對象之存儲信息區段資料單位用以生成存儲信息核對值，藉由用以執行生成後之存儲信息核對值之核對處理，用以執行前述資料中之存儲信息區段資料單位的正常性驗證處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理裝置，係根據驗證對象之存儲信息區段資料用以生成存儲信息中間值，並對生成後之存儲信息中間值適用存儲信息核對值生成驗證後用以執行驗證處理並用以生成存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，前述

五、發明說明 (45)

資料處理方法，其特徵為：係使驗證對象之存儲信息區段資料被破壞化時，藉由該存儲信息區段資料之譯碼處理將取得譯碼文全體以預定組元單位進行逐段之譯碼處理並用以生成存儲信息中間值，使驗證對象之存儲信息區段資料未被破壞化時，將存儲信息區段資料全體以預定組元單位進行預定之譯碼處理用以生成存儲信息中間值。

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵為：在前述中間值對值的生成處理進行前述預定之譯碼處理係根據逐段驗證和後之值。

進而，本發明之資料處理方法之一實施態樣中，在前述存儲信息中間值之生成處理，其特徵為：使驗證對象之存儲信息區段資料被破壞化時適用於存儲信息中間值生成處理之前述譯碼處理，係藉由C/B模式之譯碼處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：藉由前述C/B模式之譯碼處理構成，係根據在生成驗證對象之信息列的一部分被適用複數次不同驗證和後之值。

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵為：在存儲信息區段資料含有複數之零件，並使被含於該存儲信息區段資料一部分之零件未被破壞化時，根據驗證對象零件用以生成存儲信息核對值，並藉由用以執行生成後之存儲信息核對值的核對處理，用以執行前述資料中之各存儲信息區段資料單位的正常性驗證處理。

五、發明說明 (45)

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵為：在前述存儲信息同步資料包含有複數之零件，使驗證對象之要驗證零件有1個時，使前述要驗證零件未被破壞化時，藉由要驗證零件之譯碼處理將取得譯碼文全體以預定組元單位進行逐段驗證和後之值，適用存儲信息核對值生成驗證後用以執行驗證處理並用以生成存儲信息核對值，從而前述驗證零件未被破壞化時，將該要驗證零件全體以預定組元單位進行逐段驗證和後之值，適用前述存儲信息核對值生成驗證後用以執行驗證處理並用以生成存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，在前述資料處理方法，其特徵為：係在前述存儲信息同步資料包含有複數之零件，使驗證對象之要驗證零件有複數時，在各零件適用存儲信息核對值生成驗證後用以執行驗證處理取得後之零件核對值的邏輯處理，進而適用前述存儲信息核對值生成驗證後用以執行驗證處理將取得結果做為存儲信息核對值。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係進而，在被執行正常性驗證後之存儲信息區段資料舍用以收納存儲信息資料的步驟。

進而，本發明之資料處理方法之一實施態樣中，前述資料處理方法，係進而，在存儲信息核對值之核對處理中，在未來成立核對後之情形，其特徵為：前述控制部，係用以中止容納處理到前述記錄裝置。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係進而，在被執行正常性驗證後之存儲信息區段資料舍用以收納存儲信息資料的步驟。

五、發明說明⁽⁴⁵⁾

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係進而，舍用以再被執行正確性驗證後之資料用以執行再處理之步驟。

進而，本發明之資料處理方法之一實施態樣中，前述資料處理方法，係在存儲信息核對值之核對處理中，在未成立該核對值之情形中，其特徵為：用以中止再產生處理。

進而，本發明之第 2 個方面，係一種存儲信息資料驗證賦予方法，為了存儲信息資料驗證處理之存儲信息資料驗證賦予方法，其特徵為：在結合於資料驗證對象之存儲信息資料單位用以生成存儲信息核對值，並將生成後之存儲信息核對值結合驗證對象存儲信息區資料賦予存儲信息資料。

進而，本發明之存儲信息資料驗證賦予方法之一實施態樣中，其特徵為：前述存儲信息核對值，係經形成驗證對象之存儲信息區資料作為信息，適用存儲信息核對值生成論理藉由驗證處理生成之值。

進而，本發明之存儲信息資料驗證賦予方法之一實施態樣中，其特徵為：前述存儲信息核對值，係根據驗證對象之存儲信息同步資料用以生成存儲信息中間值，對該存儲信息中間值適用前述存儲信息核對值生成論理後用以執行驗證處理生成之值。

進而，本發明之存儲信息資料驗證賦予方法之一實施態樣中，其特徵為：前述存儲信息核對值，係對驗證對象之存儲信息區資料採 CBC 模式藉由用以執行暗號

五、發明說明⁽⁴⁵⁾

處理生成之值。

進而，本發明之存儲信息資料驗證賦予方法之一實施態樣中，其特徵為：係在存儲信息區資料包含有複數之零件，將結合於該存儲信息區資料一部分之零件作為驗證對象時，該驗證對象等零件用以生成存儲信息核對值，並將生成後之存儲信息核對值結合驗證對象存儲信息區資料賦予存儲信息資料。

進而，本發明之存儲信息資料驗證賦予方法之一實施態樣中，其特徵為：在前述存儲信息區資料包含有複數之零件，使驗證對象之要驗證零件有 1 個時，使前述要驗證零件被暗號化時，藉由要驗證零件之暗碼處理將該暗碼明文全體以預定固定單位在進行於暗碼化後之值，適用存儲信息核對值生成論理後用以執行暗碼處理並用以生成存儲信息核對值，並將生成後之存儲信息核對值結合驗證對象存儲信息同步資料賦予存儲信息資料。

進而，本發明之存儲信息資料驗證賦予方法之一實施態樣中，其特徵為：係在前述存儲信息同步資料包含有複數之零件，使驗證對象之要驗證零件有複數時，在各零件適用存儲信息核對值生成論理後用以執行暗碼處理對取得之零件核對值的暗碼資料，進而適用前述存儲信息核對值生成論理後用以執行暗碼處理並將取得暗碼值作為存儲

五、發明說明⁽⁵⁰⁾

信息核對值，將生成後之存儲信息核對值結合驗證對象存儲信息同步資料賦予存儲信息資料。

進而，本發明之第 2 個方面，

係一種驗證處理裝置，用以提供電腦程式藉由記憶媒體或網路提供存儲信息資料之處理在電腦系統上執行的型式而提供硬體，其特徵在於：前述電腦程式，係含有：在結合於資料驗證對象之存儲信息同步資料單位用以生成存儲信息核對值的步驟；及藉由用以執行生成之存儲信息核對值的核對處理，用以執行前述資料中之存儲信息同步資料單位的正確性驗證處理之步驟。

進而，本發明之第 2 個方面，

係一種資料處理裝置，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行生成存儲信息資料之處理的資料處理裝置，而該記錄資料處理裝置，

係對前述記錄裝置使形成存儲信息資料，將前述存儲信息資料之暗號化 Kcd 藉由暗號化 Kcd 進行暗碼處理後之暗號化資料 Kdis (Kcon) 藉由進行容納到前述集管部後之資料被構成的情形中，其特徵在於其構成具有：

將前述暗號化資料 Kdis (Kcon) 由前述集管部進行取出用以執行暗碼處理並用以生成暗碼資料 Kcon，而對該生成後之暗碼資料 Kcon 適用不同暗號化 Kstr 藉由用以執行

五、發明說明⁽⁵¹⁾

暗碼處理，根據暗號化 Kstr 用以生成暗碼處理後之新的暗號化資料 Kdis 並用以執行容納到前述存儲信息資料之集管部的處理。

本發明之第 2 個方面，

係一種資料處理裝置，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行生成存儲信息資料之處理的資料處理裝置，而前述資料處理裝置，

係對前述記錄裝置使結合於形成容納對象之存儲信息資料的前述存儲信息區段，藉由暗號化 Kcd 被暗碼化後之存儲信息，及根據暗號化 Kcon 藉由被暗碼化後之暗號化資料 Kcon (Kdis) 被構成，進而，構成有暗碼化暗號 Kcon 藉由暗號化 Kdis 消進行暗碼處理後之暗號化資料 Kdis (Kcon) 容納到前述集管部之情形中，其特徵在於其構成具有：

將前述暗號化暗號 Kdis (Kcon) 由前述集管部進行取出用以執行暗碼處理並用以生成暗碼資料 Kcon，而對該生成後之暗碼資料 Kcon 適用不同暗號化 Kstr 藉由用以執行暗碼處理，根據暗碼化 Kstr 用以生成暗碼處理後之暗號化資料 Kdis 並用以執行容納到前述存儲信息資料之集管部的處理。

進而，本發明之第 2 個方面，

係一種資料處理裝置，具有使至少一部分之區段被暗

五、發明說明(52)

號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行生成容納資料之處理的資料處理裝置。

而該裝置資料處理裝置。

係對該記錄裝置形成於形成容納對象之存儲信息資料的前述存儲信息區段，藉由暗號編碼 Kblc 被暗號化後之存儲信息，及根據暗號編碼 Kdis 藉由暗號化後之暗號編碼資料 Kdis (Kblc) 被編碼之情形中，其特徵在於其構成具有：

將前述暗號編碼資料 Kdis (Kblc) 由前述集管部進行取出，用以執行該暗號編碼 Kblc 譯碼處理並用以生成譯碼資料 Kblc，而對該生成後之譯碼資料 Kblc 適用不同暗號編碼 Kstr 藉由用以執行暗號處理，根據暗號編碼 Kstr 用以生成暗號處理後之暗號編碼 Kstr (Kblc) 並用以執行容納其存儲信息區段的處理。

進而，本發明之第 2 個實施例，

係一種存儲信息資料生成方法，用以生成存儲信息資料之存儲信息資料生成方法。

藉由含聲音資訊、影像資訊、程式資料至少其中之一資料用以複數區段連續被構成之存儲信息區段。

將複數的複數之存儲信息區段至少一部分的存儲信息區段藉由暗號編碼 Kcon 藉由暗號處理。

將暗號編碼 Kcon 藉由暗號編碼 Kdis 用以生成暗號處理後之暗號編碼資料 Kdis (Kcon) 並容納於前述存儲信息區段。

五、發明說明(53)

息資料之集管部。

並用以生成複數的存儲信息區段及集管部的存儲信息資料。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵為：前述存儲信息資料之集管部，存儲信息資料之資料長度，存儲信息資料之資料長度以容納含有無源存儲信息區段之資料長度，暗號處理之資訊後用以生成區段處理，並容納於前述集管部之處理。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵為：前述存儲信息資料生成方法，係進而，根據前述集管部之一部分資訊用以生成部分核對值，並將該部分核對值容納於前述集管部，進而，根據該部分核對值用以生成核對值，並容納於該核對值容納於前述集管部之處理。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵為：前述部分核對值之生成處理及核對值之生成處理，係將形成核對值之資料做為資訊，並將該核對值生成處理後之暗號編碼 Kdis 藉由暗號處理並進行執行。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵為：前述存儲信息資料生成方法，係進而，將前述區段資訊藉由暗號編碼 Kbit 用以暗號化處理，並將該暗號編碼 Kbit 藉由暗號編碼 Kdis 將生成後之暗號編碼資料 Kdis (Kbit) 容納於前述集管部。

五、發明說明(54)

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵為：前述存儲信息區段中之複數區段的各區段係依序而固定之資料長度並進行生成。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵為：前述存儲信息區段中之複數區段的各區段係依序而暗號化後之暗號編碼資料，及該暗號編碼資料之暗號編碼 Kblc 根據暗號編碼 Kdis 藉由暗號處理後之暗號編碼資料 Kdis (Kblc) 之相加以構成。

進而，本發明之第 2 個實施例，

係一種存儲信息資料生成方法，用以生成存儲信息資料之存儲信息資料生成方法。

藉由含聲音資訊、影像資訊、程式資料至少其中之一存儲信息區段進行複數區段連續，同時，

將複數的存儲信息區段至少一部分之區段，將含聲音資訊、影像資訊、程式資料至少其中之一之資料以暗號編碼 Kblc 將進行暗號化後之暗號編碼資料，及該暗號編碼資料之暗號編碼 Kblc 根據暗號編碼 Kdis 藉由暗號處理後之暗號編碼資料 Kcon (Kblc) 之相加以構成。

並將前述暗號編碼 Kcon 藉由暗號編碼 Kdis 用以生成暗號處理後之暗號編碼資料 Kdis (Kcon) 並容納於前述存儲信息資料之集管部。

而用以生成複數的存儲信息區段及集管部的存儲信息資料。

進而，本發明之第 3 個實施例，

係一種存儲信息資料生成方法，用以生成存儲信息資料

五、發明說明(55)

料之存儲信息資料生成方法。

將含聲音資訊、影像資訊、程式資料至少其中之一存儲信息區段進行複數區段連續，同時，

將複數的存儲信息區段至少一部分之區段，將含聲音資訊、影像資訊、程式資料至少其中之一之資料以暗號編碼 Kblc 將進行暗號化後之暗號編碼資料，及該暗號編碼資料之暗號編碼 Kblc 根據暗號編碼 Kdis 藉由暗號處理後之暗號編碼資料 Kdis (Kblc) 之相加以構成。

而用以生成複數的存儲信息區段及集管部的存儲信息資料。

進而，本發明之第 3 個實施例，

係一種資料處理方法，具有使至少一部分之區段被暗號化後之複數的存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行容納資料之處理的資料處理裝置。

對該記錄裝置形成於形成容納對象之存儲信息資料，將前述存儲信息區段之暗號編碼 Kcon 藉由暗號編碼 Kdis 藉由暗號處理後之暗號編碼資料 Kdis (Kcon) 藉由容納於前述集管部之資料被構成之情形中，其特徵在於：

將前述暗號編碼資料 Kdis (Kcon) 由前述集管部取出用以執行暗號處理並用以生成暗號編碼資料 Kcon。

對生成後之暗號編碼資料 Kcon 適用不同暗號編碼 Kstr 並藉由用以執行暗號處理，根據暗號編碼 Kstr 用以生成暗號處理後之暗號編碼資料 Kstr (Kcon)。

五、發明說明(90)

該存儲信息資料之無管資訊用以取得存儲信息資料之構成資訊並進行存儲信息資料之解析。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：在前述無管資訊，係包含應儲存信息之再生優先順位資訊，在前述仲長處理部中使形成仲長處理對象之應儲存信息有數個時，則前所述仲長處理部，係在前述存儲信息資料解析部根據被取後之無管資訊中的優先順位資訊，依從該優先順位以執行順序存儲信息仲長處理之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係進而，具有：顯示裝置，用以顯示形成仲長處理對象之應儲存信息之資訊；及輸入裝置，由該顯示於前述顯示裝置後之存儲信息資訊以輸入被選擇後之再生存儲信息識別資料；而前述仲長處理部，係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之應儲存信息之仲長處理之構成。

進而，本發明之第3至5例。

係一種資料處理裝置，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的再生處理之資料處理裝置，其特徵在於：

用以檢取出應儲存信息，或仲長處理方式其中之一之存儲信息資料，由該檢出檢取存儲信息之無管資訊從應儲存信息資料用以判別應儲存信息或仲長處理方式

本國際式進項申請中國專利權案(CNSDAI 468(2007) 056) - 63 -

五、發明說明(91)

· 同時

使該存儲信息資料有應儲存信息時，由該存儲信息資料之無管資訊，用以取得該應儲存信息之應儲存處理方式。

並具有：存儲信息資料解析部，使該存儲信息資料具有仲長處理方式時，由該存儲信息資料之無管資訊用以取得仲長處理方式；及

仲長處理部，用以執行應儲存信息之仲長處理；

藉由該仲長處理部，其構成具有：

從前述存儲信息資料解析部對解析後之應儲存信息之應儲存處理方式判斷時可使用之仲長處理方式，藉由前述存儲信息資料解析部根據被解析後之仲長處理方式判斷進行選擇，藉由該選擇後之仲長處理方式用以執行仲長處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係進而其構成具有：資料記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之應儲存信息；及程式記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之仲長處理方式；而前述仲長處理部，係根據記憶於前述資料記憶部後之應儲存信息，適用該記憶於前述程式記憶部後之仲長處理方式並用以仲長處理。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：在前述無管資訊，係包含應儲存信息之再生優先

本國際式進項申請中國專利權案(CNSDAI 468(2007) 056) - 64 -

五、發明說明(92)

該位資訊，使形成仲長處理對象之應儲存信息有數個時，則在前述仲長處理部中之存儲信息仲長處理，係在前述存儲信息資料解析部中根據被取後之無管資訊中的優先順位資訊，依從該優先順位以執行順序存儲信息之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：前述資料處理裝置，係具有檢索裝置用以檢索仲長處理方式，而前述檢索裝置，對前所述存儲信息資料解析部後之應儲存信息根據可適用之仲長處理方式，使前述資料處理裝置可存取之方式容納與應檢索對象進行檢索之構成。

進而，本發明之資料處理裝置之一實施態樣中，其特徵為：

前述資料處理裝置，係進而，具有：顯示裝置，用以顯示形成仲長處理對象之應儲存信息之資訊；及輸入裝置，由該顯示於前述顯示裝置後之存儲信息資訊以輸入被選擇後之再生存儲信息識別資料；而前述仲長處理部，係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之應儲存信息之仲長處理之構成。

進而，本發明之第3至7例。

係一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料的再生處理之資料處理方法，其特徵在於：

存儲信息資料解析步驟，含根據後之存儲信息及該

本國際式進項申請中國專利權案(CNSDAI 468(2007) 056) - 65 -

五、發明說明(93)

應儲存信息之仲長處理方式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料判斷存儲信息，及仲長處理方式之抽出處理；及

仲長處理步驟，係為前述存儲信息資料解析之解析結果使用被檢出被取後之存儲信息資料之仲長處理方式用以執行被檢出於存儲信息資料之應儲存信息之仲長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，其構成係進而具有：資料記憶步驟，藉由前述存儲信息資料解析步驟用以容納被抽出後之應儲存信息；及程式記憶步驟，藉由前述存儲信息資料解析部用以容納被抽出後之仲長處理方式；而前述仲長處理步驟，係根據記憶於前述資料記憶步驟後之應儲存信息，在前述前述程式記憶步驟中適用被記憶後之仲長處理方式並用以執行仲長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述存儲信息資料解析步驟，係根據檢出於前述存儲信息資料之無管資訊用以取得存儲信息資料之構成資訊並進行存儲信息資料之解析。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：在前述無管資訊，係包含應儲存信息之再生優先順位資訊，在前述仲長處理部中使形成仲長處理對象之應儲存信息有數個時，則前述仲長處理部，係在前述存儲信息資料解析部中根據被取後之無管資訊中的優先

本國際式進項申請中國專利權案(CNSDAI 468(2007) 056) - 66 -

A7
B7

五、發明說明(64)

取出資訊，依從該優先順位用以執行順序存儲信息伸長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係透過，具有：顯示步驟，顯示伸長處理對象之壓縮存儲信息的資訊顯示於顯示裝置；及輸入步驟，由該顯示於前述顯示裝置後之存儲信息資訊用以輸入該選擇後之再生存儲信息識別資料；而前述伸長處理步驟，係在前述輸入步驟根據輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的伸長處理。

進而，本發明之第38個圖。

係一個資料處理方法，藉由從媒體或通訊網路進行被提供之存儲信息資料之再生處理之資料處理方法，其特徵在於：

用以接收含壓縮存儲信息，或伸長處理資訊其中之一之存儲信息資料，由該含該接收存儲信息資料之集管理資訊從該存儲信息資料用以判別該存儲信息伸長處理資訊，同時，

從該存儲信息資料有壓縮存儲信息時，由該存儲信息資料之集管理資訊，用以取得該被接收存儲信息後之壓縮處理資訊，並具有：

存儲信息資料解碼步驟，從該存儲信息資料有伸長處理資訊時，由該存儲信息資料之集管理資訊用以取得伸長處理資訊；

本願式係適用中國國家專利法(CNSIA)條第(2)項(207公案) - 67 -

A7
B7

五、發明說明(65)

選擇步驟，在前述存儲信息資料解碼步驟中對解碼後之壓縮存儲信息的壓縮處理資訊種類將可適用之伸長處理資訊，藉由該被存儲信息資料解碼步驟根據該解碼後之伸長處理資訊種類加以選擇；及

伸長處理步驟，在前述選擇步驟中藉由選擇後之伸長處理資訊用以執行伸長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係適用具有：資料記憶步驟，藉由前述存儲信息資料解碼步驟用以將該被抽出後之壓縮存儲信息；及程式記憶步驟，藉由前述存儲信息資料解碼步驟用以將該被抽出後之伸長處理資訊；而前述伸長處理步驟，係在前述資料記憶步驟對該記憶後之壓縮存儲信息，並前述程式記憶步驟中適用該記憶後之伸長處理資訊並用以伸長處理。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：在前述集管理資訊，係包含壓縮存儲信息之再生優先順位資訊，以形成伸長處理對象之壓縮存儲信息有複數時，則在前述伸長處理步驟，係在前述存儲信息資料解碼步驟中根據被接收後之集管理資訊中的優先順位資訊，依從該優先順位進行順序執行。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係適用具有被集管理資訊以從集管理資訊處理資訊，而前述被集管理資訊，在前述存儲信息資料解碼步驟中對進行解碼後之壓縮存儲信息種類將可適用之伸

本願式係適用中國國家專利法(CNSIA)條第(2)項(207公案) - 68 -

A7
B7

五、發明說明(66)

與處理資訊，將可存取之程式提供被提供被集管理對象進行擴展。

進而，本發明之資料處理方法之一實施態樣中，其特徵為：前述資料處理方法，係適用具有：顯示步驟，將伸長處理對象之壓縮存儲信息的資訊顯示於顯示裝置；及輸入步驟，由該顯示於前述顯示裝置後之存儲信息資訊用以輸入該選擇後之再生存儲信息識別資料；而前述伸長處理步驟，係在前述輸入步驟根據輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的伸長處理。

進而，本發明之第39個圖。

係一個存儲信息資料生成方法，藉由從媒體或通訊網路進行被提供之存儲信息資料之生成處理之存儲信息資料生成方法，其特徵為：

用以生成被該壓縮後之存儲信息資訊及該壓縮存儲信息之伸長處理資訊組合的存儲信息資料。

進而，本發明之存儲信息資料生成方法之一實施態樣中，進而其特徵為：係為前述存儲信息資料之集管理資訊用以附加該存儲信息資料之構成資訊。

進而，本發明之存儲信息資料生成方法之一實施態樣中，進而其特徵為：係為前述存儲信息資料之集管理資訊，係用以附加被包含於該存儲信息資料之存儲信息之再生優先順位資訊。

進而，本發明之第40個圖。

本願式係適用中國國家專利法(CNSIA)條第(2)項(207公案) - 69 -

A7
B7

五、發明說明(67)

係一個存儲信息資料生成方法，藉由從媒體或通訊網路進行被提供之存儲信息資料之生成處理之存儲信息資料生成方法，其特徵為：

從存儲信息資料用以判別該壓縮存儲信息或伸長處理資訊之存儲信息資料種類與集管理資訊並進行附加。

從該存儲信息資料係壓縮存儲信息時，則將該被適用於該壓縮存儲信息後之壓縮處理資訊種類做為集管理資訊並進行附加。

而從該存儲信息資料係伸長處理資訊時，則將伸長處理資訊種類做為集管理資訊並用以生成附加後之存儲信息資料。

進而，本發明之存儲信息資料生成方法之一實施態樣中，其特徵為：係為前述存儲信息資料之集管理資訊，係用以附加被包含於該存儲信息資料之存儲信息之再生優先順位資訊。

進而，本發明之第41個圖。

係一個程式提供資訊，用以以該電腦程式藉由記憶媒體或通訊網路將該提供存儲信息資料之再生處理在電腦系統上執行的程式提供資訊，其特徵在於：前述電腦程式，係具有：

存儲信息資料解碼步驟，含被該解碼後之存儲信息資訊及該壓縮存儲信息之伸長處理資訊用以執行存儲信息資料之存儲信息資料解碼，並用以執行由該存儲信息資料之壓縮存儲信息，及伸長處理資訊之抽出處理；及

本願式係適用中國國家專利法(CNSIA)條第(2)項(207公案) - 70 -

A7
B7

五、發明說明(68)

伸長處理步驟，做為前述存儲信息資料解碼之解碼結果使用被用於取得後之存儲信息資料的伸長處理程序用以執行被用於該存儲信息資料之壓縮存儲信息的伸長處理。

有關本發明之程式提供媒體，係譬如，再獲運之程式代碼對可執行的汎用電腦系統，將電腦程式以電腦可讀之形式並行提供之媒體，係CD或FD、MO等之記憶媒體，或，網路等之傳送媒體等，其形態並無特別限定。

如此之程式提供媒體，係在電腦系統上為用以實現預定之電腦程式的功能，用以定義電腦程式及提供媒體之構造上或功能上協同性關係，換言之，透過該媒體提供再擴展程式或由安裝於電腦系統，在電腦系統上被選擇協同性作用，可取得與本發明其他例同樣的作用效果。

本發明適用於其他目的，特徵或優點，係根據後述之本發明實施例或後述方式藉由更詳細之說明成為更明確吧！

【發明之實施形態】

以下用以說明本發明之實施形態，說明之順序，係根據以下之項目進行。

- (1) 資料處理裝置構成
- (2) 存儲信息資料形式
- (3) 資料處理裝置中之可適用之暗號處理機能
- (4) 記錄再生部之存儲資料構成

本發明式適用於中國國家標準 (GB2818 規格 (2007 年)) - 71 -

A7
B7

五、發明說明(69)

(5) 記錄裝置之存儲資料構成

- (6) 記錄再生部，記錄裝置間中之相互認證處理
- (6-1) 相互認證處理之概要
- (6-2) 相互認證時之暗號處理的切換
- (7) 由記錄再生部到記錄裝置之下載處理
- (8) 以記錄裝置存儲資訊之記錄再生部之再生處理
- (9) 相互認證後之暗號交換處理
- (10) 運載之存儲信息資料形式，及對應於各形式之下載及再生處理

(11) 存儲信息供應者中之後對值 (ICV) 生成處理關係

- (12) 根據主暗號之所選處理暗號生成構成
- (13) 暗號處理中之暗號識別控制
- (14) 根據存儲信息資料中之處理方針中之暗號處理先順位之程式暗號處理
- (15) 存儲信息構成及再生 (伸長) 處理
- (16) 存儲資料之生成及對記錄裝置的存儲，再生處理
- (17) 不正當暗號之防偽構成
- (18) 安全晶片構成及製造方法

(1) 資料處理裝置構成

圖2係顯示有關本發明之資料處理裝置之一實施例全體構成方塊圖，本發明之資料處理裝置，係對記錄再生部

本發明式適用於中國國家標準 (GB2818 規格 (2007 年)) - 72 -

A7
B7

五、發明說明(70)

300及記錄裝置400做為主要構成要素。

記錄再生部300，係譬如藉由個人電腦 (PC: Personal Computer)，或遊戲機等被構成，記錄再生部300，係如圖2所示，具有：控制部301，用以執行該控制部301所控制之300中暗號處理時之記錄裝置400均造控制，記錄再生部暗號處理部302，管理暗號處理全部；記錄裝置控制部303，透過對記錄再生部暗號處理部302用以執行暗號處理並進行資料之讀出；讀取部304，由DVD等之媒體至少進行資料之讀出；及通訊部305，與外部進行資料之收發。

記錄再生部300，係藉由控制部301之控制對記錄裝置400之存儲信息資料之下載，由記錄裝置400用以執行存儲信息資料再生，記錄裝置400，係對記錄再生部300載往係可讀之記錄媒體，譬如記憶卡等，具有外部記憶體402藉由EEPROM、閃光記憶體等之非易失記憶體，硬盤、附屬RAM等被構成。記錄再生部300，係具有：讀取部304，將該等讀取部2之左端所示之記憶媒體，DVD、CD、FD、HD後之存儲信息資料做為可讀口；及通訊部305，由網際網路等之網路被配對存儲信息資料做為可輸入的接口；由外部用以輸入存儲信息。

記錄再生部300，係具有暗號處理部302，透過讀取部304或通訊部305藉由外部被輸入之存儲信息資料在記錄裝置400進行下載處理時，或將存儲信息

本發明式適用於中國國家標準 (GB2818 規格 (2007 年)) - 73 -

A7
B7

五、發明說明(71)

藉由記錄裝置400再生，進行執行時之暗號處理，暗號化處理，暗碼化處理，進而用以執行資料之暗號處理等，暗號處理部302，其構成係具有：控制部300，用以控制暗號處理部302；內部記憶部307，用以保持暗號處理時之暗號等之資訊，並由外部裝置不尋常使資料讀出之媒體；及暗碼／暗碼化部308，進行暗號化處理，暗碼化處理，暗碼用之資料之生成，亂數之產生等。

控制部301，係譬如，在記錄再生部300被裝有記錄裝置400時透過記錄裝置控制部303發送初始化指令到記錄裝置400，或，在記錄再生部暗號處理部302之時點／暗碼化部406之間進行在相互認證處理，係對暗碼化處理，暗號化，暗碼化處理等，在各種處理中進行分步處理，對於此等各處理，在後段加以詳細說明。

暗號處理部302，係如前所述用以執行暗號處理，暗號化處理，暗碼化處理，進而資料之暗號處理等之處理部，具有暗碼處理控制部306，內部記憶部307，暗碼／暗碼化部308。

暗號處理控制部306，係在記錄再生部300中被執行有關暗號處理，暗碼／暗碼化處理等之暗號處理並用以執行控制之控制部，譬如，在記錄再生部300及記錄裝置400之間被執行暗號處理之時，將暗碼化處理之設定，記錄再生部暗號處理部302之時點／暗碼化部308中執行各種處理，譬如下載，或有關再生

本發明式適用於中國國家標準 (GB2818 規格 (2007 年)) - 74 -

AT
BT

五、發明說明(72)

存儲信息資料之核對係生成處理之執行指令，各種輸出之生成或處理的執行指令等，進行有關時處理信息的控制。

內部記憶體307，係在後續加以詳細說明，但在記錄再生部300被執行相互認證處理，核對值被核對處理，暗號化，譯碼化，譯碼化處理等，在各種處理形成必要之暗號資料，或用以印製類別資料等。

暗號/譯碼化部308，係使用被寄附於內部記憶體307之後的暗號資料等，由外部被輸入將存儲信息資料在記錄裝置400進行下載處理時，或將被寄附於記錄裝置400之後的存儲信息資料由記錄裝置400進行再生，執行時之認證處理，暗號化處理，譯碼化處理，進而用以執行預定之核對值或電子署名之生成，驗證，資料之驗證，異數之產生等的處理。

此外，記錄再生部300與部302之內部記憶體307，係為了用以保持暗號化部等之重要之資訊，係由外部有必要難以不正當讀出之構造。因此，暗號處理部302，係由外部以有難難以存取構造之半導體晶片被構成，具有多層構造，其內部記憶體係被嵌於絕緣層之層層，或在絕緣層被構成，又，進行動作之電壓或/且從頻率之寬頻狹窄等，由外部具有難以不正當資料讀出之特性使其與暗號化部或電子署名之生成，驗證，資料之驗證，異數之產生等的處理。

記錄再生部300，係除了此等之暗號處理功能之外，具備有：中央演算處理裝置(主CPU：Central

本圖式係說明本發明實施例之構成(圖1) (200頁) - 75 -

AT
BT

五、發明說明(73)

Processing Unit) 108、RAM(Random Access Memory) 107、ROM(Read Only Memory) 108、AV處理部109、輸入接口110、PIO(並聯I/O接口) 111、SIO(串聯I/O接口) 112。

中央演算處理裝置(主CPU：Central Processing Unit) 106、RAM(Random Access Memory) 107、ROM(Read Only Memory) 108，係作為記錄再生部300本體之控制系統或驅動部之構成部，並作為記錄再生部暗號處理部302用以執行暗號化後之資料再生後再再生處理發揮功能，譬如中央演算處理裝置(主CPU：Central Processing Unit) 106，係在控制部301之控制下由記錄裝置被讀出被暗號化後之存儲信息資料進行輸出到AV處理部109等，進行有關存儲信息之再生，執行之控制。

RAM107，係作為CPU106中之各種處理用的主記憶體或緩衝器使用，藉由CPU106為了處理成為存儲區域被使用。ROM108，係以主CPU108被動為了上述OS等被動的基本程式等。

AV處理部109，具體而言，係如具有MPEG2解碼器、AT-TRAC解碼器、MPS譯碼器等之資料處理部或處理部，對付於記錄再生部本體被讀出之未處理之資料或解碼器等之資料輸出機器用以執行為了資料輸出之處理。

輸入接口110，係由遙控器等之控制部，鍵盤，滑

本圖式係說明本發明實施例之構成(圖2) (200頁) - 76 -

AT
BT

五、發明說明(74)

鼠等，各種之輸入裝置所輸入資訊輸出到主CPU106，主CPU106，係如根據執行中之選單格式等由使用者從控制部依從指示用以執行處理。

PIO(並聯I/O接口) 111，SIO(串聯I/O接口) 112，係為記憶卡、磁碟卡等之記憶裝置，備用電子機器等做為附加接口被使用。

又，主CPU106，係如具有有關執行中之選單等設定資料等做為安全資料記憶於記錄裝置400時也進行控制。在該處理時，係將記憶資料轉送到控制部301，控制部301係根據必要在暗號處理部302與有關安全資料之暗號處理部執行，並將暗號化資料寄附於記錄裝置400，對於此等之暗號處理，係在後續加以詳細說明。

記錄裝置400，係如前記被供於記錄再生部300可拆卸之記憶裝置，譬如藉由記憶卡被構成，記錄裝置400係具有暗號處理部401，外部記憶體402。

記錄裝置暗號處理部401，係由記錄再生部300之存儲信息資料的下載，或由記錄裝置400對記錄再生部300之存儲信息資料的再生處理時等中之記錄再生部300及記錄裝置400間的相互認證處理，暗號化處理，譯碼化處理，進而用以執行資料之驗證處理等的處理部，而記錄再生部300之暗號處理部具有有關暗號控制部，內部記憶體，暗號/譯碼化部等，此等之暗號處理部係於圖3、外部記憶體402，係如前述，譬如由EEPROM等

本圖式係說明本發明實施例之構成(圖3) (200頁) - 77 -

AT
BT

五、發明說明(75)

之光記錄裝置所構成字串與記憶體，藉由磁頭，附帶RAM等被構成，並用以容納暗號化後之存儲信息資料。

圖3係顯示本發明之資料處理裝置由接收資料供給之存儲信息記憶裝置的圖500。通訊裝置600被輸入之資料構成暗號裝置，同時由此等存儲信息提供裝置500，600用以輸入存儲信息並將暗號化後之資料300，及記錄裝置400中之暗號處理的構成從中心，顯示其構成。

裝置500，係如圖光碟裝置，磁碟裝置，磁帶裝置，半導體裝置等，通訊裝置600，係如網路裝置，通訊裝置，衛星通訊等，可資料通訊之裝置。

圖3中，記錄再生部300，係由存儲信息提供裝置之裝置500，通訊裝置600被輸入之資料，即如圖3所示依從預定之形式用以驗證存儲信息，並在驗證後將存儲信息係存於記錄裝置400。

如圖3之裝置500，通訊裝置600部分所示存儲信息資料係具有如下之構成部，具有：

類別資訊：做為存儲信息資料之類別子之類別資訊。

處理方針：做為存儲信息資料之構成資訊，譬如用以構成存儲信息資料之存儲部或區域，存儲信息區域，存儲之方式，使存儲部或顯示方式或資料之存儲信息形式，進而使存儲信息係以圖3所示之機器可利用或與其他機器也可利用等之限制利用資訊等之處理方針。

本圖式係說明本發明實施例之構成(圖4) (200頁) - 78 -

A7

B7

五、發明說明 (76)

區段資訊 由顯示存儲信息區段、區段標格、暗號化之有無的暗號化標記等構成之區段資訊。

鑰匙資料 由用以暗號化上述區段資訊之暗號化鑰匙、或用以暗號化存儲信息區段之存儲信息鑰匙等所構成之鑰匙資料。

存儲信息區段 由形成資訊之再生對象之格式資料、管理、鑰匙資料所成存儲信息區段。

尚有，對於存儲信息資料之詳情，係在後段使用圖4以下而詳細加以說明。

存儲信息資料 係指由存儲信息鑰匙（於此，係將此稱為存儲信息鑰匙（Content Key（以下，做爲 Kcon）））暗號化、由媒體500、通訊裝置600被提供到記錄再生部300、存儲信息、係通過記錄再生部300可存取於記錄裝置400之外部記憶體。

譬如，記錄裝置400，係使用收容於記錄裝置內之內部記憶體405後之記錄裝置管理有鑰匙（於此，係將此稱為存儲鑰匙（Storage Key（以下，做爲 Kstr））），包含於存儲信息資料之存儲信息、及做爲存儲信息資料之無管理資訊包含有之區段資訊、各種鑰匙資訊、譬如用以暗號化存儲信息鑰匙 Kcon 等並進行記憶於外部記憶體402，由存儲信息資料之記錄再生部300下處理後到記錄裝置400，或經由記錄再生部300被收納於記錄裝置400內之存儲信息資料的再生處理中，係使被區分之相互暗號處理、存儲信息資料之暗號化、譯碼化處理等，形

本國際大體適用中國專利審查規則 (CNDA) 規格 (210+297) 公證。 -79-

A7

B7

五、發明說明 (77)

成必要預定之手續，對於此等之處理，係在後段加以詳細說明。

記錄裝置400，係如圖3所示具有暗號處理部401、外部記憶體402、暗號處理部401、係具有部403、通訊部404、內部記憶體405、暗號／譯碼化部406、及外部記憶體控制部407。

記錄裝置400，係管理暗號處理部401，用以限制外部記憶體402，同時由記錄再生部300用以解釋指令，由用以執行處理之記錄裝置暗號處理部401，及用以保持存儲信息等之外部記憶體402所構成。

記錄裝置暗號處理部401，係具有：控制部403，用以限制記錄裝置暗號處理部401全體、通訊部404，與記錄再生部300進行資料之收發；內部記憶體405，用以保持暗號處理用之鑰匙資料等之資訊，並由外部不可寫入出處理；暗號／譯碼化部406，進行暗號化處理、譯碼化處理、認證用之資料的生成、驗證、亂數之產生等；及外部記憶體控制部407，用以限制外部記憶體402之資料。

控制部403，係在記錄裝置400中用以執行有關被執行之暗號處理、暗號化／譯碼化處理等之暗號處理全體的處理。譬如，在記錄再生部300及記錄裝置400之間被執行之暗號處理終了時之暗號終了暗號之設定、暗號處理部401之暗號／譯碼化部406之被執行之各種處理、譬如下記，及有將再生存儲信息資料之被

本國際大體適用中國專利審查規則 (CNDA) 規格 (210+297) 公證。 -80-

A7

B7

五、發明說明 (78)

新發生處理之執行指令，各種鑰匙資料之生成處理的執行指令等，進行有關暗號處理全體的處理。

內部記憶體405，係在後段加以詳細說明，但係由具有暗號之區段記錄裝置402，在記錄裝置400中被執行之相互暗號處理、暗號化處理、暗號化處理、暗號化處理等，在各處理形成必要之鑰匙資料、或形成用以被數帶關鍵別資料等之構成。

記錄裝置暗號處理部401之內部記憶體405，係與前段說明之記錄再生部暗號處理部302之內部記憶體307同樣，爲了用以保持暗號處理等之必要資訊，由外部有必要形成以不正當讀出之構造。因此，記錄裝置400之暗號處理部401，係由外部以具有鑰匙以存取構造之中間體晶片被構成，並具有多種構造，其內部之記憶體被塗於記憶等之裝置，或塗於被塗下，又，被動作之電壓及／或頻率之資訊被讀取，被構成或經由外部難以不正當資料讀出之特性。尚有，記錄再生部暗號處理部302，係保持鑰匙等之秘密資訊可存取範圍到外部被構成之狀態也可。

暗號／譯碼化部406，係由記錄再生部300之存儲信息資料的下載處理，被收容於記錄裝置400之外部記憶體402後之存儲信息資料的再生處理、或記錄再生部300及記錄裝置400間之相互暗號處理時，使用被收容於內部記憶體405後之鑰匙資料等，用以執行資料之暗號處理、暗號化處理、譯碼化處理、預定之暗號處理

本國際大體適用中國專利審查規則 (CNDA) 規格 (210+297) 公證。 -81-

A7

B7

五、發明說明 (79)

電子等名的生成、驗證及亂點之產生等的處理等。

通訊部404，係根據接收於記錄再生部300之記錄裝置控制部303，依從記錄再生部300之控制部301，或記錄裝置400之控制部403，進行存儲信息資料之下載處理、再生處理、或、相互暗號處理時之記錄再生部300及記錄裝置400間的轉送資料之通訊。

(2) 存儲信息資料格式

其次，使用圖4乃至圖8，對於被收容於本發明之系統中之媒體500，或用以通訊資料是記錄裝置600之資料格式加以說明。

圖4所示之構成係顯示存儲信息資料全體之格式圖，圖5所示之構成係顯示用以構成存儲信息資料之無管理的一部分「處理方針」之詳細圖，圖6所示之構成係顯示用以構成存儲信息資料之無管理的一部分「區段資訊」之詳細圖。

尚有，於此，係對於本發明系統中被適用之資料格式的代表性之一例加以說明，但本發明之系統，係可對於除於本說明書之格式，適用於含資料等之實際處理的格式等，被不同種類之資料格式可利用，對於此等之格式之關係，係在後段「(10) 被數之存儲信息資料格式」及對應於各格式之下載及再生處理中，更詳細地說明。

圖4所示資料格式中，以灰色顯示部分係被暗號化後之資料，二重框部分係被收發對資料，其他之白色部分係

本國際大體適用中國專利審查規則 (CNDA) 規格 (210+297) 公證。 -82-

AT

BT

五、發明說明 (80)

未將暗號化平本文之資料、暗號化部之暗號化輸出、係分別顯示於右之左邊的輸出。圖4所示例中，係在存儲信息部之各區段（存儲信息區段資料）與在被暗號化之區段及未被暗號化之區段、此等之形態，係根據存儲信息資料不同的形態，使適合於資料全部之存儲信息區段資料被暗號化的構成也可。

如圖4所示，資料格式，係按成分集管理部及存儲信息部，集管理，係藉由區段資訊（Content ID）、處理方針（Usage Policy）、核對值A（Integrity Check Value A（以下，做為ICV a））、區段資訊輸出（Block Information Table Key（以下，做為Kbit））、存儲信息輸出Kcon、區段資訊（Block Information Table（以下，做為BIT））、核對值B（ICV b）連續排列（ICV t）被構成，而存儲信息部，係由被暗號化之存儲信息區段（譬如被暗號化後之存儲信息，及未被暗號化之存儲信息）被構成。

於此，區別資訊，係顯示了用以區別存儲信息之區別資訊（Content ID）、處理方針，係如圖5所示之狀態，而顯示被管理部分之大小之區段大小（Header Length），顯示存儲信息部分之大小之存儲信息大小（Content Length），顯示格式之方案資訊的格式方案（Format Version），顯示格式之區段的格式區段（Format Type），顯示被保存於存儲信息部之存儲信息係何種，或資料等存儲信息之類別的存儲信息型態（Content Type），存儲

AT

BT

五、發明說明 (81)

注意區段係顯示式時之移動優先權位的移動優先權位資訊（Operation Priority），依從該格式被下載後之存儲信息，僅能利用下載後之機器，或顯示也可利用其他同樣機器的限制利用資訊（Localization Policy），依從該格式被下載後之存儲信息，顯示由下載後之機器是否在其他同樣的機器可複製之複製限制資訊（Copy Permission），依從該格式被下載後之存儲信息，顯示由下載後之機器是否在其他同樣的機器可移動之移動限制資訊（Move Permission），用以暗號化存儲信息部內之存儲信息區段而顯示使用之算法的暗號化算法（Encryption Algorithm），用以暗號化存儲信息部內之存儲信息區段而顯示使用之算法的使用方法之暗號化格式（Encryption Mode），顯示被暗號化之生成方法的驗證方法（Integrity Check Method）被構成。

尚有，記錄於上述之處理方針的資料項目，係1項之例，根據對應之存儲信息資料的態樣用以記錄權限之處理方針資訊，譬如在後段之「(17)不正當權限之排除資訊」加以詳細說明，僅將不正當之記錄再生的識別子進行記錄，藉由利用開始與之限制由於不正當權限能用以排除存儲信息利用之構成也可。

核對值A、ICV a，係為了用以驗證區段資訊，處理方針之資訊的核對值，並非存儲信息資料全部係部分資料之核對值，即做為部分核對值發揮功能，資料區段資訊輸出Kbit，係用以暗號化區段資訊而被使用，而存儲信

AT

BT

五、發明說明 (82)

是輸出Kcon，係用以暗號化存儲信息區段而被使用，尚有，資料部區段資訊輸出Kbit及存儲信息輸出Kcon，係在區段500上及區段資訊600上係以後述之配適輸出（Distribution Key（以下，做為Kdis））被暗號化。

將區段資訊之詳細顯示於右，尚有，圖6之區段資訊，係由圖4被暗號化後由全部資料區段資訊輸出Kbit被暗號化之資料、區段資訊，係如圖6所示，而顯示存儲信息區段之數的存儲信息區段數（Block Number）及N個之存儲信息區段資訊被構成。存儲信息區段資訊，係由區段大小（Block Length）、顯示是否被暗號化之暗號化標誌（Encryption Flag），顯示是否有必要用以計算核對值的驗證資訊標誌（ICV Flag），存儲信息核對值（ICV i）被構成。

存儲信息核對值，係為了用以驗證各存儲信息區段之資訊被使用之核對值，對於存儲信息核對值之生成方法的具體例，係在後段「(10)複製之資料格式」及對應於各格式下載處理到記憶裝置及由記憶裝置之再生處理之圖加以說明，尚有，將區段資訊進行暗號化之資料區段資訊輸出Kbit，係通過，藉由配適輸出Kdis被暗號化。

繼續圖4之資料格式的說明，核對值B、ICV b，係為了用以驗證區段資訊輸出Kbit，存儲信息輸出Kcon，區段資訊之資訊的核對值，並非存儲信息資料全部而係部分資料之核對值，即做為部分核對值發揮功能，核對值ICV t，係為了用以資訊ICV a、ICV b，各形

AT

BT

五、發明說明 (83)

係由區段資訊之核對值ICV i（被設定之情形），此等之部分核對值，或形成核對值對象之資料全部的核對值。

尚有，圖6中，將區段大小，暗號化標誌，驗證對象標誌自由可設定，但做為某種程度限制之構成也可，譬如，將暗號化區域及平常文檔處理區域區段大小，或將全部存儲信息資料行暗號化，用以區段區段資訊BIT也可，又，將存儲信息輸出Kcon在各存儲信息區段為了形成不同，將存儲信息輸出Kcon並對在區段部分，便合於存儲信息區段也可，對於存儲信息資料格式之例，係在「(10)複製之存儲信息資料格式」及對應於各格式下載及再生處理之項目中，加以詳細說明。

(3) 本發明之資料處理裝置中可適用之暗號處理概要

其次，對於本發明之資料處理裝置中被適用取得之各種暗號處理的態樣加以說明，尚有，系顯示於本項目「(5) 本發明之資料處理裝置中可適用之暗號處理之概要」之暗號處理的說明，係在後段以及圖加以說明本發明之資料處理裝置中之各種處理，譬如a、記錄再生的及記錄裝置間之區段處理、b、對於存儲信息之記錄裝置的下載處理、c、對於於記錄裝置後之存儲信息的再生處理等處理中對於被執行形成處理處理之暗號處理的態樣，將此態樣加以說明，對於記錄再生300及記錄裝置400中之具體性處理，係在本說明書之項目(4)以下，對於各處理詳細加以說明。

A7
BT

五、發明說明 (84)

以下，對於資料處理裝置中之可通用的暗號處理之概要。

- (3-1) 藉由公開鍵暗號方式之信息認證
- (3-2) 藉由公開鍵暗號方式之電子署名
- (3-3) 藉由公開鍵暗號方式之電子署名的驗證
- (3-4) 藉由公開鍵暗號方式之相互認證
- (3-5) 公開鍵暗號證書
- (3-6) 藉由公開鍵暗號方式之相互認證
- (3-7) 使用兩組由該暗號之暗號化處理
- (3-8) 使用兩組由該暗號之暗號化處理
- (3-9) 亂數產生裝置

之順序加以說明。

(3-1) 藉由公開鍵暗號方式之信息認證

首先，對於使用公開鍵暗號方式後之取改檢測資料的生成處理加以說明。取改檢測資料，係對於欲進行取改之檢測的資料，為了用以取改之檢對及作成否認證的資料。

譬如，在圖4已說明之資料構造中之二重複部分之各該對值A、B，根據對值，及圖6所示使該等於該區段資訊中之各區段後之存留信息核對值，做為該取改檢測資料生成。

於此，係做為電子署名的生成處理方式之一使用公開鍵暗號方式中之DES例加以說明。尚有，本發明中

A7
BT

五、發明說明 (85)

，係DES之外，也可使用同樣做為公開鍵暗號方式中之取改檢測DES (Fast Encipherment Algorithm: NTT)，AES (Advanced Encryption Standard: 英國大開羅暗號) 等。

將使用一般性的DES之電子署名的生成方式使用圖7加以說明。首先，先行用以生成電子署名，將形成電子署名之對數個容進行分割成8組元單位(以下，將被分割後之信息做為M1、M2、...MN)，而且，將最初期(Initial Value (以下，稱為IV))及M1進行排他性邏輯和(將其結果做為I1)。接著，將I1及M2進行排他性邏輯和，並將其輸出I2輸入到DES暗號化部，使用暗號K1進行暗號化(輸出E2)，以下將此處理，對全部之信息實施暗號化處理，在最後出現之EN成為電子署名。該值一般係稱為信息認證符號(MAC (Message Authentication Code))，被使用於信息之取改檢對。又，將此使用暗號化處理方式稱為CCB (Cipher Block Chaining) 模式。

尚有，如圖7之生成例中被輸出之MAC值，係圖4所示資料構造中之二重複部分之各該對值A、B，根據對值，及被取改等於圖6所示區段資訊中之各區段的存留信息核對值ICV1~ICVN可適用。在該MAC值之檢正時，係使該值與生成時同樣之方式用以生成MAC值，能取得同一之值時，則能將暗號化成功。

尚有，圖7所示之演算係初期值IV，在最初之8組

A7
BT

五、發明說明 (86)

先信息M1進行排他性邏輯和之後，做為初期值Y=0，但將初期值也可做為非排他性邏輯和之構成。

對圖7所示MAC生成方法，進而將顯示提高安全性之MAC生成方法的處理構成圖顯示於圖8。圖8係顯示取代圖7之單DES使用三倍DES (Triple DES) 用以執行MAC值之生成例。

將圖8所示各三倍DES (Triple DES) 構成部之群組構成例示於圖9。如圖9(a)，(b)所示做為三倍DES (Triple DES) 之構成例具有二例之不同構成。圖9(a)，係顯示使用2個之暗號暗號之構成，藉由暗號1進行暗號化處理，藉由暗號2進行暗號化處理，進而藉由暗號1進行暗號化處理之順序處理。暗號1，係使用K1、K2、K1之順序2個，圖9(b)係顯示使用3個之暗號暗號之構成，藉由暗號1進行暗號化處理，藉由暗號2進行暗號化處理，進而藉由暗號3進行暗號化處理之順序處理進行3次暗號化處理。暗號1，係使用K1、K2、K3之順序3個，如此使連續暗號化處理之構成，此單DES使安全性提高。可見，該三倍DES (Triple DES) 構成，係使處理時暗號化DES之三倍之缺點。

將用以改良圖8及圖9說明之三倍DES構成例

MAC值生成構成例顯示於圖10。圖10中，係由形成署名對象之信息列的數列於途中停止對各信息之暗號化處理全部部暗號化DES做為處理，僅對最後之信息的暗號化處理進行圖9所示三倍DES (Triple DES) 構成。

A7
BT

五、發明說明 (87)

做為如圖10所示之構成，僅係MAC值之生成處理時間，係根據DES與MAC值生成處理所需時間大略同程度被短縮，且安全性係藉由三倍DES比MAC值可更高。尚有，對該信息之三倍DES構成，係可認為圖9(b)之構成。

(3-2) 藉由公開鍵暗號方式之電子署名

以上，係做為暗號化方式適用公開鍵暗號暗號化方式之情形之電子署名資料之生成方法，但其次，將做為暗號化方式使用公開鍵暗號暗號化方式之電子署名生成方式使用圖11加以說明。圖11所示處理，係使用EC-DSA (Elliptic Curve Digital Signature Algorithm)，IEEE P1363/D3之電子署名資料之生成處理構成。尚有，於此係做為公開鍵暗號暗號化方式使用橢圓曲線暗號化(Elliptic Curve Cryptography (以下，稱為ECC))之例加以說明。尚有，本發明之資料處理裝置中，除了橢圓曲線暗號化之外，也同樣在公開鍵暗號暗號化方式中，譬如也可使用RSA暗號化(Rivest, Shamir, Adleman)等(ANSI X9.31))。

對於圖11之各步驟加以說明。在步驟S1中，將p做為模數，a、b為橢圓曲線之係數(橢圓曲線： $y^2 = x^3 + ax + b$)，G為橢圓曲線上之基點，r為G之倍數，K為橢圓曲線暗號化($0 < K < r$)。在步驟S2中，用以計算信息M之亂數(Hash值)H，做為f =

AT
BT五、發明說明⁽⁸⁸⁾

Hash (M)。

於此，使用亂數函數將求出亂數值方法加以說明，所謂亂數函數，係將信息做為輸入，並將此壓縮成預定之位元長的資料，做為亂數值進行輸出之函數。亂數函數，係由亂數值（輸出）用以再回輸入為循環，使被輸入於亂數函數之後的資料的1位元進行變化時，使亂數值之許多位元產生變化，又，具有找出具有同一亂數值不同的輸入資料為困難之特徵。故稱亂數函數，也有強硬用MD4，MD5，SHA-1等之情形，該情形，係形成最後輸出值MAC（供對值，相當於ICV）成為亂數值。

接著，在步驟S3，用以生成亂數 u ($0 < u < r$)，並在步驟S4將該點用以計算進行 u 倍之後的座標 V (Xv, Yv)，所有，應由曲線上之加算，2倍係例如下所述。

【數1】

$$\begin{aligned} \text{做爲 } P &= (Xa, Ya) \cdot Q = (Xb, Yb) \cdot R \\ &= (Xc, Yc) = P + Q \end{aligned}$$

P+Q時（加算）

$$Xc = A^2 \cdot Xa - Xb$$

$$Yc = \lambda \times (Xa - Xb) - Ya$$

$$\lambda = (Yb - Ya) / (Xb - Xa)$$

$$P \cdot Q \text{ 時 (2倍算)}$$

$$Xc = \lambda^2 - 2Xa$$

$$Yc = \lambda \times (Xa - Xc) - Ya$$

此種說明書係根據日本特許廳公佈之專利文件

本願書式適用中國專利審查標準 (CN2004/2127) (2007) (公案) - 91 -

AT
BT五、發明說明⁽⁸⁹⁾

$$\lambda = (3(Xa)^2 + a) / (2Ya)$$

使用此等用以計算點 G 之 u 倍（速度慢，但較為容易了解之演算法係如下進行，用以計算 $G \cdot 2 \times G \cdot 4 \times G \dots$ ，將 u 進行2進位數展開用以加算對應於使1成立時之 $2^i \times G$ （將 G 進行 i 次2倍算之值）（ i 係由 u 之LSB數時之位元位置）。

在步驟S5，用以計算 $K = Xv \bmod r$ ，在步驟S6用以判定該值是否為0，若非0則在步驟S7用以計算 $d = [(f + cKs) / u] \bmod r$ ，並在步驟S8用以判定 d 是否為0，若 d 非0，則在步驟S9將 c 及 d 做為電子署名資料進行輸出。如果，將 r 假定做為160位元長之長度，則電子署名資料係形成320位元長。

在步驟S6中，使 c 為0時，則返回到步驟S3用以生成並修正的亂數。同樣，在步驟S8使 d 為0時，也返回到步驟S3用以生成並修正亂數。

(3-3) 藉由公開鍵點加算方式之電子署名的驗證

其次，將使用公開鍵點加算方式之電子署名的驗證方法，使用圖12加以說明。在步驟S11，將 M 做為信息， p 為模數， a, b 為橢圓曲線之係數（橢圓曲線： $y^2 = x^3 + ax + b$ ），將 G 為橢圓曲線之上點， r 為 G 之位數， G 及 $K \times G$ 為公開鍵點（ $0 < K < r$ ），在步驟S12使電子署名資料 c 及 d 用以驗證是否為 $0 < c < r$ ， $0 < d < r$ ，將此滿足時，則在步驟S13，用以計

此種說明書係根據日本特許廳公佈之專利文件

本願書式適用中國專利審查標準 (CN2004/2127) (2007) (公案) - 92 -

AT
BT五、發明說明⁽⁹⁰⁾

算信息 M 之亂數值，做為 $f = \text{Hash}(M)$ ，其次，在步驟S14用以計算 $h1 = d \bmod r$ ，並在步驟S15用以計算 $h1 = f \bmod r$ ， $h2 = c \bmod r$ 。

在步驟S16中，使用已經計算之 $h1$ 及 $h2$ ，用以計算點 $P = (Xp, Yp) = h1 \times G + h2 \cdot Ks \times G$ ，電子署名驗證者，係已知有公開鍵點 G 及 $Ks \times G$ ，所以與 $h1$ 之步驟S4同樣可計算橢圓曲線上之點的座標。而且，在步驟S17用以判定點 P 是否為該點，即非無該點則進到步驟S18（實際上，無該點之判定係在步驟S16可進行，總之，進行 $P = (X, Y) \cdot Q = (X, -Y)$ 之加算，則使 Y 不能計算，則 $P + Q$ 在無限遠點）。在步驟S18用以計算 $Xp \bmod r$ ，並與電子署名資料進行比較。在最後，使該值一致時，則進到步驟S19，判定電子署名係正確。

係判定電子署名係正確後，資料係不能篡改，可知用以保持對應於公開鍵點之秘密點係用以生成電子署名。

在步驟S12中，使電子署名資料 c 或 d ，未滿足 $0 < c < r$ ， $0 < d < r$ 時，則進到步驟S20。又，在步驟S17中，點 P 在無限遠點時也進到步驟S20。進到又，在步驟S18中，使 $Xp \bmod r$ 之值，未與電子署名資料 c 一致時也進到步驟S20。

在步驟S20中，被判定電子署名不正當時，資料係

此種說明書係根據日本特許廳公佈之專利文件

本願書式適用中國專利審查標準 (CN2004/2127) (2007) (公案) - 93 -

AT
BT五、發明說明⁽⁹¹⁾

被篡改，但可用以保持對應於公開鍵點之秘密點係用以生成電子署名。

(3-4) 藉由共同點加算方式之相互驗證

其次，將使用共同點加算方式之相互驗證方法，使用圖13加以說明。在圖13中，做為共同點加算方式使用有DES，但知知該等有同樣之共同點加算方式則皆可。圖13中，首先，使 B 用以生成64位元之亂數 Rd ，並將 Rb 及自己之ID的ID(b)發送到 A ，將此接收後之 A ，使用以生成新的64位元之亂數 Ra ，並與 $Ra, Rb, ID(b)$ 之順序，以DES之CBC模式使用點 Kab 用以加密化資料，並逐逐到 B ，若依排圖7所示DES之CBC模式處理構成，則相當於 Ra 為 $M1, Rb$ 為 $M2, ID(b)$ 為 $M3$ ，而初期值： $IV = 0$ 時使輸出 $E1, E2, E3$ 成為暗號文。

將此接收後之 B ，係將接收資料以點 Kab 進行譯碼化，接收資料之譯碼化方法，係首先，將暗號文 $E1$ 以點 Kab 進行譯碼化，取得亂數 Ra ，其次，暗號文 $E2$ 以點 Kab 進行譯碼化，並與結果將 Rb 進行排他邏輯和，取得 Rb ，最後，暗號文 $E3$ 以點 Kab 進行譯碼化，並與結果將 $E2$ 進行排他邏輯和，取得ID(b)，如此被取得之 $Ra, Rb, ID(b)$ 之內，便及 b 及ID(b)，用以驗證是否與發送的資料一致，通過該驗證時，則保持 A 做為真正資料加以認證。

此種說明書係根據日本特許廳公佈之專利文件

本願書式適用中國專利審查標準 (CN2004/2127) (2007) (公案) - 94 -

A2
B2五、發明說明⁽⁹²⁾

接著B，係在認證使用以生成（生成方法，係使用亂數）使用之對照時間點（Session Key（以下，做爲Kses）），而且，以Rb、Ra、Kses之順序，以DBS之CBC模式使用輸出Ka b進行雜質化，並輸出至A。

將此接收後之A，係將接收資料以輸出Ka b進行雜質化，接收資料之雜質化方法，係與B之雜質化處理相同，所以在此省略詳細說明。如此接收後之Ra、Rb、Kses之間，使Rb及Ra，用以驗證A是否與前述的進行一致，透過該驗證時，則A係將B做爲正當並加以認證。在相互用此認證力之後，對該時間點Kses，係係利用做爲認證後之秘密通訊用之共同輸出。

尚有，在接收資料之驗證時，检测到不正當，不一致時，則做爲相互認證失敗而予以中斷處理。

(3-5) 公開輸出證明書

其次，對於公開輸出證明書使用圖14加以說明，公開輸出證明書，係公開輸出時點方式之認證局（CA：Certificate Authority）進行發行的證明書，使用者將自己之ID，公開輸出證等經由內部證局提出，認證局側用以附加認證局之ID或有效期限等資訊，進而根據認證局用以附加簽名後作成之證明書。

圖14所示公開輸出證明書，係含證明書之方案號碼，認證局對證明書利用者分發的證明書號碼，使用於電子署名之算出及參數，認證局之名稱，證明書之有效期限，

本國際式進用中國國家標準（CNS/A4規格（210×297公厘））—95—

A2
B2五、發明說明⁽⁹³⁾

證明書利用者之名稱（利用者ID），證明書利用者之公開輸出及電子署名。

電子署名，係對證明書之方案號碼，認證局對證明書利用者分發的證明書號碼，使用於電子署名之算出及參數，認證局之名稱，證明書之有效期限，證明書利用者之名稱及證明書利用者之公開輸出全體應用亂數函數生成以生成亂數值，對該亂數值係使用認證局之秘密輸出證生成後之資料，該電子署名之生成，係係利用該證明書11說明之處理流程。

認證局，係進行發行圖14所示公開輸出證明書，而時更新有效期限與輸出之公開輸出證明書，爲了進行排斥進行不正當行為之利用者作成不正當者名單，進行管理，配布（請此關係者取消：Revocation），又，根據必要也進行公開輸出，秘密輸出之生成。

另外，在利用該公開輸出證明書時，利用者係使用自己採行之認證局的公開輸出，用以驗證該公開輸出證明書之電子署名，在電子署名之輸出進行成功之後由公開輸出證明書取出公開輸出，並利用該公開輸出，因此，利用公開輸出證明書之所有利用者，係有必須保持共同之認證局的公開輸出，所有，對於電子署名之驗證方法，係在圖12已說明所以省略其詳細說明。

(3-6) 藉由公開輸出時點方式之相互認證

其次，將使用公開輸出時點方式之160位元長之真

本國際式進用中國國家標準（CNS/A4規格（210×297公厘））—95—

A2
B2五、發明說明⁽⁹⁴⁾

藉由輸出時點相互認證方法，使用圖15加以說明，圖15中，係將公開輸出時點方式係使用RCC，係如前述與以同樣之公開輸出時點方式對等可。又，輸出大小也非160位元不可，圖15中，首先係B，用以生成64位元，並發送給A，將此接收後之A，係用以生成剩余的比64位元之亂數Ra及模數p更小的亂數Ak，而且，將該點G求出進行A k參照之點Av=A k×G，對Ra、Rb、Av（X座標及Y座標）用以生成電子署名A、Sig，並與A之公開輸出證明書一起運送到B，於此Ra及Rb分別有64位元，Av之X座標及Y座標分別有160位元，所以對合計448位元用以生成電子署名。電子署名之生成方法係在圖11已說明，所以省略其詳細說明。又，公開輸出證明書也在圖14已說明，所以省略其詳細說明。

接收A之公開輸出證明書，及Ra、Rb、Av、電子署名A、Sig後之B，係使A進來之Rb，用以驗證是否與B生成的一致，其結果，進行一致時，則將A之公開輸出證明書內的電子署名以認證局之公開輸出進行驗證，並取出A之公開輸出，對於公開輸出證明書之驗證，係使用圖14已說明，所以省略說明，而且，使用取出的A之公開輸出用以驗證電子署名A、Sig，電子署名之驗證方法係在圖12做了說明，所以省略其說明，在電子署名之驗證進行成功之後，B係將A做爲正當者加以認證。

本國際式進用中國國家標準（CNS/A4規格（210×297公厘））—97—

A2
B2五、發明說明⁽⁹⁵⁾

其次，B係用以生成比模數p更小的亂數Bk，而且，將該點G求出進行B k倍之點Bv=B k×G，對Ra、Rb、Bv（X座標及Y座標）用以生成電子署名B、Sig，並與B之公開輸出證明書一起運送到A。

接收B之公開輸出證明書，及Ra、Rb、Av、電子署名B、Sig後之A，係使B進來之Ra，用以驗證是否與A進行生成的一致，其結果，進行一致時，則將B之公開輸出證明書內的電子署名以認證局之公開輸出進行驗證，並取出B之公開輸出，而且，使用取出的B之公開輸出用以驗證電子署名B、Sig，在電子署名之驗證進行成功後，A係將B做爲正當者加以認證。

使用上述認證進行成功時，則B係用以計算B k×Av（B k倍亂數，但Av係因爲在橢圓曲線上之點，所以必要橢圓曲線上之點的標量值計算），而A係用以計算Ak×Bv，並對此等之X座標的下方64位元做爲對該時間點並使用於以後之通訊（將公開輸出證明書做爲64位元輸出之共同輸出時間點時），當然，由Y座標用以生成對該時間點輸出，亦，非下位64位元也可，尚有，相互認證後之秘密通訊中，發送資料係不僅以對該時間點輸出驗證，也係利用有電子署名。

在電子署名之驗證或接收資料之驗證時，發現不正當，不一致時，則做爲相互認證進行失敗而予以中斷處理。

(3-7) 使用橢圓曲線時點之時點化處理

本國際式進用中國國家標準（CNS/A4規格（210×297公厘））—98—

AT
BT

五、發明說明 (95)

其次，對於使用橢圓曲線暗號之時號化，使用圖16加以說明。步驟S21中，將 $M \times X$ 、 $M \times Y$ 做為舊信息，將 p 為舊數， a 、 b 為橢圓曲線之係數（橢圓曲線： $y^2 = x^3 + ax + b$ ），將 G 為橢圓曲線上之基點，將 t 為 G 之位數，將 G 及 $K \times G$ 為公開鍵點（ $0 < K < r$ ），在步驟S22用以生成亂數 u 成為 $0 < u < r$ ，並在步驟S23將公開鍵點 $K \times G$ 用 u 計算進行 u 倍之座標 V 。接著，橢圓曲線上的座標係在圖11之步驟S24已做說明，所以省略其說明。在步驟S24，將 V 之座標進行 M 倍以 p 求出剩餘值為 $X0$ ，在步驟S25將 V 之 Y 座標進行 $M \times Y$ 倍以 p 求出剩餘值為 $Y0$ 。倘有，使信息之座標比 p 之位元數見小時，則 $M \times Y$ 係使用亂數，在譯碼化部係用以解密 $M \times Y$ 。在步驟S28中，用以計算 $u \times G$ ，並在步驟S27取得暗號文 $u \times G$ 、 $(X0, Y0)$ 。

(3-3) 使用橢圓曲線暗號之譯碼處理

其次，使用橢圓曲線暗號之譯碼化，使用圖17加以說明。在步驟S31中，將 $u \times G$ 、 $(X0, Y0)$ 做為暗號文資料，將 p 為舊數， a 、 b 為橢圓曲線之係數（橢圓曲線： $y^2 = x^3 + ax + b$ ），將 G 為橢圓曲線上之基點，將 t 為 G 之位數，將 K 為秘密鍵點（ $0 < K < r$ ），在步驟S32中，將暗號文和 $u \times G$ 進行秘密鍵點 K 倍，以求出座標 $V(XV, YV)$ 。在步驟S33，係將暗號文內，用以取出 $(X0, Y0)$ 之座標，並用

AT
BT

五、發明說明 (97)

以計算 $X1 = X0 / YV \bmod p$ ，在步驟S34中，係用以 Y 座標，用以計算 $Y1 = Y0 / YV \bmod p$ 。而且，在步驟S35將 $X1$ 做 $M \times X$ ，並將 $Y1$ 做為 $M \times Y$ 用以取出信息。此時，將 M 本進行信息時， $Y1$ 係進行解密。

因此，將秘密鍵點為 $K \times G$ ，公開鍵點為 G ，以做為 $K \times G$ ，將使用於暗號化之鍵點及用於譯碼化之鍵點，可視為不同鍵點。

又，經由公開鍵點暗號之其他例係已知有RSA，但省略詳細說明（在PKCS#1 Version2被詳述）。

(3-9) 亂數生成處理

其次，對於亂數之生成方法加以說明，做為亂數之生成方法，已知有用以放大熱雜音，由其 A/D 進行生成之真性亂數生成法，或將 M 系列等之變形電路裡數組合進行生成之擬真亂數生成法等。又，也已知有使用DES等之共同鍵點暗號進行生成之方法，以本例，係對於使用DES之擬真亂數生成法加以說明（ANSI X9.17基準）。

首先，由時間等之資料將被取得之84位元（以下之位元數之情形，將上位元做為0）之值做為 D ，將使用於Triple-DES之鍵點資訊做為 $K1, K2$ ，將亂數產生用之種（Seed）做為 S 。此時，亂數 R 係以如下被計算。

$$I = \text{Triple-DES}(K(K(K, D)) \dots (2-1))$$

$$R = \text{Triple-DES}(K(K, S^1)) \dots (2-2)$$

AT
BT

五、發明說明 (98)

$$S = \text{Triple-DES}(K(K, R^1)) \dots (2-3)$$

除此，Triple-DES，係將第1引數做為暗號化資訊，將第2引數之值以Triple-DES做為進行暗號化之函數，將第3引數64位元單位之排他性座標和，在最後出現之值 S ，係做為新的Seed（種）並做為鍵更新。

以下，用以生成進行座標之亂數時，係將(2-2)式，(2-3)式重複進行。

以上，本發明之資料處理裝置中對於有能可適用的暗號處理態樣做了說明。其次，本發明之資料處理裝置中對於被執行之具體性的處理，詳細加以說明。

(4) 記錄再生器之容納資料構成

圖18係用以說明以圖3所示記錄再生器300在記錄再生器暗號處理部302被讀取後之內部記錄體307的資料保持內容。

如圖18所示，在內部記錄體307，係包含有以下之機能，資料。

MkRe：在記錄再生器300及記錄裝置400（參考圖3）之間在被執行之相互認證處理為用以生成必要的認證鍵（Authentication and Key Exchange Key（以下，做為Ksk））之記錄裝置認證用光暗號。

VkRe：記錄裝置認證暗號用初期值。

MKdis：為了用以生成記錄鍵Kdis之記錄暗號用主鍵點。

AT
BT

五、發明說明 (99)

Vdis：記錄暗號生成用初期值。

Kieva：為了用以生成核對值ICV a之暗號的核對值A生成暗號點。

Kicvb：為了用以生成核對值ICV b之暗號的核對值B生成暗號點。

Kieva：為了用以生成容納信息資訊之核對值ICV i（ $i = 1 \sim N$ ）之暗號的容納信息核對值A生成暗號點。

Kicvi：為了用以生成核對值ICV t之暗號的核對值B生成暗號點。

Ksys：在配訊系統為附加上共同之署名或ICV使用之系統署名暗號點。

Kdev：在各記錄再生器不同，為了使記錄再生器附加上署名或ICV使用之記錄再生器固有之記錄再生器署名暗號點。

Ivmen：被使用於初期值，相互認證處理等時之暗號處理的初期值，暗號裝置共同。

此等之暗號，資料係被容納於被構成在記錄再生器暗號處理部302的內部記錄體307。

(5) 記錄裝置之容納資料構成

圖19係顯示記錄裝置上資料保持狀況圖。圖19中，內部記錄體405，係被分形成數之暗號（以本例係N個段），在分列之暗號中，被容納有以下之暗號，資料

A2
B2

五、發明說明(100)

Idmem：記錄裝置識別資訊，記錄裝置固有之識別資訊。

Kake：認證輸出，與記錄再生器300使用於相互認證之認證輸出。

Ivmem：新關係，相互認證處理時等被使用時被處理部402之初期值。

Kstr：保存輸出，該資訊除其他存儲信息資料之輸出輸出。

Kr：亂數生成亂數。

S：值。

將此等之資料各自保持於個別之區域，外部記憶體402係用以保持該數（以本例係M個）之存儲信息資料，分別以圖4將已說明之資料，譬如保持於如圖26，或圖27，對於圖26，圖27之構成之器具係在後再加以說明。

(6) 記錄再生器，記錄裝置間之相互認證處理

(6-1) 相互認證處理之概要

圖20係顯示記錄再生器300及記錄裝置400之認證程序流程圖，在步驟S41中，使用者將記錄裝置400插入到記錄再生器300，使以非接觸方式使用通訊記錄裝置時，不必進行插入。

在記錄再生器300用以設定記錄裝置400，則使

本國際公開說明書中圖樣與圖表(CNS/A4規格(210×297公厘)) - 105 -

A2
B2

五、發明說明(101)

圖3所示記錄再生器300內之記錄裝置識別資訊（未表示），將記錄裝置400之裝置進行通知到控制部301。其次，在步驟S42中，記錄再生器300之控制部301，係透過記錄裝置識別部303用以發送初始化指令將記錄裝置400，將此接收後之記錄裝置400，係在記錄裝置識別部401之控制部403，透過通訊部404用以接收指令，並將該接收了有被設定到進行消除，即設定於未認證狀態。

其次，步驟S44中，記錄再生器300之控制部301，係使用記錄裝置400之記錄裝置識別部401用以指定輸出號碼，向有，有關係部從該部之評價值後送，步驟S45中，記錄再生器300之控制部301，係讓出該部存儲於記錄裝置400之內部位記憶405被指定之輸出號碼後之記錄裝置識別資訊Idmem，在步驟S46中，記錄再生器300之控制部301，係發送記錄裝置識別資訊Idmem到記錄再生器時被處理部302，並根據記錄裝置識別資訊Idmem從認證輸出Kake生成，做為認證輸出Kake之生成方法，保管如下進行生成。

【數式3】

$$Kake = DES(M(Kake, Idmem) \cdot Ivsk)$$

於此，Mkake，係在記錄再生器300及記錄裝置400（參照圖3）之間在被執行相互認證處理時用生成必要之認證輸出Kake之記錄裝置識別部主輸出，此係

本國際公開說明書中圖樣與圖表(CNS/A4規格(210×297公厘)) - 106 -

A2
B2

五、發明說明(102)

，如前所述等納於記錄再生器300之內部位記憶307，又，Idmem，係在記錄裝置400固有之記錄裝置識別資訊，進而Ivake，係記錄裝置400固有之初期值，又，在上式式中，DES()，係將第1引數做為輸入輸出，將第2引數之值以DES進行轉換化之函數，而表示供顯示64位元單位之排他性邏輯和。

譬如適用圖7，圖8所示DES構成時，則將該顯示於圖7、8之信息M做為記錄裝置識別資訊：Idmem，並將輸出K1做為認證輸出主輸出：Mkake，將初期值IV做為Ivake使被取得之輸出形成認證輸出Kake。

其次，在步驟S47進行相互認證及對話時間輸出Kstr之生成處理，相互認證，係在記錄再生器時被處理部302之輸出/譯碼化部308及記錄裝置時被處理部401之輸出/譯碼化部406之間進行，將其中介使記錄再生器300之控制部301進行。

相互認證處理，係譬如依據前圖13所說明之順序執行，圖13所示構成中，A、B係分別對應於記錄再生器300及記錄裝置400，首先，使記錄再生器300之記錄再生器時被處理部302用以生成亂數Rb，並將該亂數Rb及自己之ID之記錄再生器識別資訊IDdev發送到記錄裝置400之記錄再生器時被處理部401，向有，記錄再生器識別資訊IDdev，係記錄於被構成在記錄再生器300內之記憶部之再生器固有之識別部，在記錄再生器時被處理部302之內部位記憶中用以記錄該資訊

本國際公開說明書中圖樣與圖表(CNS/A4規格(210×297公厘)) - 105 -

A2
B2

五、發明說明(103)

再生器識別資訊IDdev做為構成也可。

接收亂數Rb及記錄再生器識別資訊IDdev後之記錄裝置400之記錄裝置時被處理部401，係用再生器識別部64位元之亂數Ra，依Ra，Rb，及記錄再生器識別資訊IDdev之順序，以DES之CBC模式使用該輸出Kake進行時被化，並發送該記錄再生器300之記錄再生器時被處理部302，譬如，若依圖7所示DES之CBC模式處理時，則相當於Ra為M1，Rb為M2，IDdev為M3，而從初期值做為：IV-Ivmem時之輸出E1，E2，E3形成被輸出。

接收被輸出E1，E2，E3後之記錄再生器300的記錄再生器時被處理部302，係將接收資料以認證輸出Kake進行譯碼化，接收資料之譯碼方法，首先，將被輸出E1以認證輸出Kake進行譯碼，將其結果及Ivmem進行排他性邏輯和，並取得輸出Ra，其次，將被輸出E2以認證輸出Kake進行譯碼化，將其結果及E1進行排他性邏輯和，取得Rb，最後，將被輸出E3以認證輸出Kake進行譯碼，將其結果及E2進行排他性邏輯和，取得記錄再生器識別資訊IDdev，如此被取得之Ra，Rb，及記錄再生器識別資訊IDdev內，使Rb及記錄再生器識別資訊IDdev，用以驗證記錄再生器300發送的是否一致，透過該驗證時，記錄再生器300之記錄再生器時被處理部302係將記錄裝置400做為正當者加以認證。

本國際公開說明書中圖樣與圖表(CNS/A4規格(210×297公厘)) - 106 -

A2
B7

五、發明說明(104)

其次，記錄再生部300之記錄再生部管理處理部302，係在認證後以生成（生成方法，係使用亂數）使用之對話時間鍵匙（Session Key（以下敘為Kses）），而且，依Rb、Ra、Kses之順序，以DES之CBC模式使用鍵匙Kake，初期值Ivmem進行暗號化，並透過記錄裝置400之記錄裝置管理處理部401。

將此暗號化之記錄裝置400之記錄裝置管理處理部401，係將接收資料以鍵匙Kake進行譯碼化，接收資料之譯碼化方法，係與記錄再生部300之記錄再生部管理處理部302中之譯碼化處理同樣，所以在此省略說明。如此被取得之Rb、Ra、Kses之間，使Rb及Ra，用以驗證暗號化裝置400發送的是否一致。通過驗證時，記錄裝置400之記錄裝置管理處理部401係將記錄再生部300敘為正常並加以認證，並相互認證對方之，則對話時間鍵匙Kses，係為了認證之秘密通訊資料而共同被能利用。

尚有，在接收資料之驗證時，發現不一致，不一致時，則使相互認證做為失敗並用其中斷處理。

在相互認證成功時，由步驟S48進到步驟S49，將對話時間鍵匙Kses以記錄再生部300之記錄再生部管理處理部302加以保存，同時將相互認證終了並用以設定記錄終了標記。又，在相互認證失敗時，則進到步驟S50，以保證處理過程用以取廢止生成後之對話時間鍵匙Kses，同時用以清除記錄終了標記，尚有已經被清除時

此圖係說明記錄再生部300之記錄再生部管理處理部302之動作。

本圖式係適用於中國專利法第33條第2項第(2)款 - 107 -

A2
B7

五、發明說明(105)

不一定需要清除處理。

尚有，使記錄裝置400由記錄裝置插入口被取出時，而使記錄再生部300內之記錄裝置管理處理部，將記錄裝置400被取出之事項通知記錄再生部300之控制部301，將此接收後之記錄再生部300之控制部301，係對記錄再生部300之記錄再生部管理處理部302將對應於記錄裝置插入口號碼之認證進行清除指令，將此接收後之記錄再生部300之記錄再生部管理處理部302，係將對應於記錄裝置插入口號碼之認證終了標記進行清除。

尚有，於此係對於相互認證處理根據圖13所示程序進行執行之敘述了說明，但不限定於上述之認證處理例，譬如用以執行根據前面說明之圖15的相互認證手續之處理也可。又，圖15所示手續中，將圖13之A敘為記錄再生部300，將B敘為記錄裝置400，使B：記錄裝置400將最初送到A：記錄再生部300之1D敘為記錄裝置中之秘密通訊資料中的記錄裝置識別資訊並進行相互認證處理也可。本發明中被執行之認證處理手續，係可選用種種之處理，並非限定於上述之認證處理。

(6-2) 相互認證時之輸出區區的特點

本發明之資料處理裝置中之相互認證處理之1個特徵，係在記錄裝置400個用以構成被認證之輸出區區（ex. N個之輸出區區），並使記錄再生部300用以指

此圖係說明記錄再生部300之記錄再生部管理處理部302之動作。

此圖係說明記錄再生部300之記錄再生部管理處理部302之動作。

本圖式係適用於中國專利法第33條第2項第(2)款 - 108 -

A2
B7

五、發明說明(106)

定（圖20之處理流程中之步驟S44）1個之輸出區區用以執行認證處理之型。如圖19所敘之說明，在使將對應於記錄裝置400之暗號化裝置401的內部記憶體405係被形成有複數之輸出區區，並分別用以收納不同的輸出區區資料，ID資訊等各種資料。在圖20已說明之記錄再生部300及記錄裝置400間被執行之相互認證處理，係對圖19之記錄裝置400之複數輸出區區之一個輸出區區被執行。

先前，用以執行認證處理及其再生機管理之相互認證處理的構成，係使用於相互認證之輸出區區認證鍵一般係被使用共同的輸出區區。因此，譬如在各製品發售對象（圖19），或在各製品欲與認證鍵匙，而在記錄再生部，及記錄裝置側之認證處理形成有必要的輸出區區資料在雙方之裝置中成為必要進行變更，因此譬如在被收納於新的被出售後之記錄再生部的認證處理形成有必要的輸出區區資料，係不屬於被收納於先被販賣之記錄裝置的認證處理形成有必要的輸出區區資料，新的記錄再生部，係將新的型式之記錄裝置形成不能存取之事項。相反地在新的型式之記錄裝置及新的型式之記錄再生部的關係也會發生同樣之事項。

本發明之資料處理裝置中，係如圖19所示與先在記錄裝置400被形成有複數之輸出區區被收納有輸出區區，記錄再生部例如各製品發售對象（圖19），或在各製品、機體、型式、應用型式，被設有應用於認證處理之輸出區區，即被設有指定輸出區區、被設定資訊，係被收納於

此圖係說明記錄再生部300之記錄再生部管理處理部302之動作。

本圖式係適用於中國專利法第33條第2項第(2)款 - 109 -

A2
B7

五、發明說明(107)

記錄再生部之記憶體部，譬如圖3中之內部記憶體307，係記錄再生部300之具有其他之記憶元件，在認證處理時藉由圖3之控制部301被存取並進行使認證裝置後之輸出區區指定。

記錄再生部300之內部記憶體307之記錄裝置部採用主輸出區區Make，係根據分別之指定輸出區區的設定被設定後之認證鍵匙應用資訊，形成可對應於指定輸出區區，形成構成指定輸出區區以外之輸出區區的相互認證不成立。

由圖19被理解，在記錄裝置400之內部記憶體405係被設定有1~N之N個輸出區區，在各輸出區區被收納有記錄裝置識別資訊，認證鍵匙，初期值，保存資訊，亂數化生成鍵匙，應，並使認證用之輸出區區資料在各輸出區區為不同資料被收納。

如此，記錄裝置400之輸出區區的輸出區區資料，係在各區區不同。因此，譬如，使記錄再生部A採用被收納於內部記憶體之記錄裝置部採用主輸出區區Make可進行認證處理之輸出區區被收納區區No. 1，又使另外規格之記錄再生部B可認證之輸出區區被收納於輸出區區，譬如即敘為設定完成輸出區區No. 2。

在後敘及更詳細加以說明，但將存儲於被收納於記錄裝置400之內部記憶體402時，使用被收納於各輸出區區被收納之保存輸出區區Katr被暗號化處理，並形成認證資訊，更與認證資訊，係將認證資訊並透過認證裝置並保存認證資訊

此圖係說明記錄再生部300之記錄再生部管理處理部302之動作。

此圖係說明記錄再生部300之記錄再生部管理處理部302之動作。

本圖式係適用於中國專利法第33條第2項第(2)款 - 110 -

五、發明說明 (108)

段以保存鐘匙進行暗號化處理。

如圖 1.9 所示保存輪匙，係在各區段被構成做為不同用途。因此，能用以指定不同輪匙區段在被指定之 2 個不同裝置的記錄再生條碼。條碼被容納於某 1 個之記錄裝置的記憶體之存儲信息被防止以兩者共同利用。即，形成不同裝置之記錄再生條碼，係符合於分別之裝置僅可利用被容納於記錄裝置後之存儲信息。

尚有，對於各輪匙區段可具同化資料係也可進行共同化，譬如僅將認證用之輪匙資料，保存輪匙資料構成不同也可。

如此在記錄裝置中造成數種不同的編碼規則用以表示產生編碼結果之具體例，僅當可對清楚指定於該發生器中 300 之機體別（裝置型、機體型等）明確指定產生編碼結果之裝置型，或在各應用程序時指定產生編碼結果之裝置型不同，從而，譬如對於在日本販賣之記錄裝置將產生指定產生編碼結果為 N 0，1，在美國販賣之記錄裝置產生碼將指定產生編碼結果為 N 0，2。依此各裝置型可構成使用不同的編碼結果設定。以如此之構成，在分別不同販賣地區使用，而在記錄裝置以不同裝置型與裝置別之存貯信息，係使用此種設定來記憶該信息而無誤讀到該信息，或由於日本與美國特殊關係，被該裝置不同編碼結果之記錄裝置不能使用，所以可防止等納於記憶裝置之存貯信息的不正確，無秩序之流通。具體而言，係以如下所保存之 Xstr 係與裝置別之存貯信息與編碼結果 2 處間可保持可靠之利用的狀態。

五、發明說明 (109)

進而，圖 19 所示記錄裝置 400 之內區記憶體 405 的編址區段 1~N 碼止之至少 1 個編址區段，譬如將 No. N 之編址區段在其中之一之記憶而生諸 300 也可做為構成共同利用之編址區段也可。

譬如，在全部之機器上輪匙點區 No. N 用以以容納可認察的記錄裝置即註用主輪匙點 Mttic，在記錄發生者 300 之範圍則，可應用程式，各節區等則以無關係值為可流過之存儲信息可應用。譬如，以容納於輪匙點區 No. N 之保存裝置裝於容納於記錄主之聯變化存儲信息，係在全部之機器中形成可利用的存儲信息。譬如將將資料等可共與可利用的之輪匙點區的存儲信息進行檢索化並記錄於記憶卡，將該記憶卡，譬如同樣使用以容納共同之記錄裝置即註用主輪匙點 Mttic 在圖帶中之裝置再生機等進行設定，由記憶卡可用以資料之傳遞與再生。

圖 2 係顯示本發明之資料庫結構圖中共有被數之論點區段的記錄裝置利用例。記錄再生器 2101 係對日本之製品的記錄再生，而在記錄裝置之論點區段 No. 1、4 之間持有主輪成立標誌區域。記錄再生器 2102 係對 US 之製品的記錄再生，而在記錄裝置之論點區段 No. 2、4 之間持有主輪成立標誌區域。記錄再生器 2103 係對 EU 之製品的記錄再生，而在記錄裝置之論點區段 No. 3、4 之間持有主輪成立標誌區域。

譬如記錄再生器 2101，係與記錄裝置 A、2104 之輸出區段 1 或輸出區段 4 之間便說成立，並

五、聲明說明 (110)

於例便實地證明。或後述之存儲係透過被寄託於論地區區
的保險庫起見並非寄託於外間。設論者生 2102，
係與保險庫 2、2105 之論地區 2 或論地區 4 之
之關係經証立。並分別便實地處理處境之存儲係透過
寄託於論地區區區的保險庫被寄託於外間即認應。設論者
生第 2103，係與保險庫區 2、2106 之論地區 3
或論地區 4 之間經証立成立，並分別便實地處理處境
之存儲係透過寄託於論地區區區的保險庫被寄託於外
間即認應。故此，再將認證人 A、2104 橫著於論地區
生第 2102，或論地區生第 2103 時，以論地區 1 之
保險庫被寄託處理處境之存儲係，供在設論者生第
2102，設論者生第 2103 及論地區 4 之間經証立
可成立或可成爲不可利用。另外，以論地區 4 之保險
庫被寄託處理處境之存儲係，供在設論者生第 2102，
設論者生第 2103 及論地區 4 之間經証立成立可成
爲可利用。

如上述，本發明之資料處理裝置中，在記錄裝置由複數之不同論點組用以構成論點區段，另外，在記錄再生機構，係對特定之論點區段用以容納可認證之主論點做為構成，所以根據價值之利用態樣可用以設定存儲信息之利用限制。

尚有，1 個之記錄再生機器中將可指定之論點區段做爲複數，譬如做爲 $1 \sim k$ ，其他之記錄再生器中將可指定之論點區段也可做爲複數如 $p \sim q$ ，又，將可共同利用之

五、發明說明 (111)

鑄造區段構成複雜也可。

(7) 由記錄再生器對記錄裝置之下載處理

其次，本發明之資料處理裝置中，對於由記錄再生器300在記錄裝置400之外部記憶體用以下載存儲信息之處理加以說明。

圖 2.2 係用以說明由記錄再生器 300 對記錄裝置 400 用以下載存儲信息之順序流程圖。倘有圖 2.2 中，係做為在記錄再生器 300 及記錄裝置 400 之間已經完成上述之相互認證處理。

步驟 S51 中，記錄再生器 300 之控制部 301，係使用讀取部 304 由用以收納存儲信息後之媒體 500 讀出依據預定之格式之資料，或接收通訊部 305 由通訊裝置 600 依據預定之格式用以播放資料。而且，記錄再生器 300 之控制部 301，係將資料內之集羣 (Header) 部分 (參閱圖 4) 發送給記錄再生器 300 之記錄再生器時裝載部 302。

其次，步驟 S52 中，在步驟 S51 用以提取集管 (Header) 後之記錄再生器暗號處理部 302 的控制部，係在記錄再生器暗號處理部 302 之暗號/譯碼化部 308 使核對值 A 計算。核對值 A，係如圖 23 所示，將被保存於記錄再生器暗號處理部 302 之內部記憶體 303 之核對值 A 生成鍵點 Kiva 值為關鍵。將該內部記憶 (Content ID) 及處理方針 (Usage Policy) 當做信息位連續了已說明

A7
B7

五、發明說明(112)

之 ICV 計算方法係計算，尚有初期值，係使為 $IV=0$ ，但在記錄再生器時處理部 302 之內部記憶體 307 用以保存核對值 A 生成用初期值 IV 放著，將此加以使用也可，最後，用以比較核對值 A 及被收納於黑窗 (Header) 內之核對值：ICV a，在進行一致後則開始到步驟 S53。

首先如圖 4 中已說明之核對值 A、ICV a，係為了用以驗證識別資訊，處理方針之複寫的核對值，將該保存於記錄再生器時處理部 302 之內部記憶體 307 的核對值 A 生成輸出 Kicva 做為輸出，將識別資訊 (Content ID) 及處理方針 (Usage Policy) 做為信息做輸出 7 已說明之 ICV 計算方法所計算所對策，但與被收納於黑窗 (Header) 內之核對值：ICV a 進行一致後時，用該判斷與對策，處理方針所更改。

其次，步驟 S53 中，記錄再生器時處理部 302 之控制部 306，係使配送輸出 Kdis 之生成在記錄再生器時處理部 302 之輸出部 308 進行，作為配送輸出 Kdis 之生成方法，係如圖 4 如下所述。

【數式 4】

$$Kdis = DES(MKdis, Content ID \oplus Vdis)$$

於此，MKdis，係為了用以生成配送輸出 Kdis 之配送輸出主輸出，此係，如前述被收納於記錄再生器 300 之內部記憶體的輸出，又 Content ID 係保存信息資料之黑窗部的識別資訊，進而 Vdis，係配送輸出用初期值，又，

本國際大元通商中韓專利權 (CN2004 專利 (2004) 第 115 號)

A7
B7

五、發明說明(113)

上述式中，DES ()，係將第 1 引數做為再輸出輸出，用以暗號化第 2 引數之值的函數，而將一係顯示 64 位元之暗號性邏輯和。

步驟 S54 中，記錄再生器時處理部 302 之控制部 306，係使用記錄再生器時處理部 302 之輸出部 308，在步驟 S53 使用生成後之配送輸出 Kdis，通過讀取部 304 接收後之復寫 500，或進行通過通訊部 305 由通訊裝置 600 收容於接收後之資料的無管部之複寫資訊輸出 Kbit 及存儲信息輸出 Kcon (參照圖 4) 之暗號化處理，如被顯示於圖 4 此等複寫資訊輸出 Kbit 及存儲信息輸出 Kcon，係在 DVD、CD 等之媒體，或網路部等之通訊路上，藉由配送輸出 Kdis 與先被資訊而暗號化處理。

進而，步驟 S55 中，記錄再生器時處理部 302 之控制部 306，係使用記錄再生器時處理部 302 之輸出部 308，在步驟 S54 以暗號化後之複寫資訊輸出 Kbit 用以暗號化複寫資訊 (BIT)，如被顯示於圖 4 此等複寫資訊 (BIT) 係在 DVD、CD 等之媒體，或網路部等之通訊路上，藉由配送輸出 Kdis 與先被資訊而暗號化處理。

進而，步驟 S56 中，記錄再生器時處理部 302 之控制部 306，係將複寫資訊輸出 Kbit，存儲信息輸出 Kcon 及複寫資訊 (BIT) 分割成 8 組元單位，將此等全部進行排他性邏輯和 (加算，減算等，其中之一減算即可

本國際大元通商中韓專利權 (CN2004 專利 (2004) 第 116 號)

A7
B7

五、發明說明(114)

其次，記錄再生器時處理部 302 之控制部 306，係在記錄再生器時處理部 302 之輸出部 308 裝核對值 B (ICV b) 計算，核對值 B，係如圖 24 所示，將該保存於記錄再生器時處理部 302 之內部記憶體 307 的核對值 B 生成輸出 Kicvb 做為輸出，將期計算後之暗號性邏輯和值以 DES 進行暗號化並加以生成，最後，用以比較核對值 B 及 Header 內之 ICV b，在進行一致後時達到步驟 S57。

如前圖 4 中已說明，核對值 B、ICV b，係為了用以驗證複寫資訊輸出 Kbit、存儲信息輸出 Kcon、複寫資訊 (BIT) 之更改的核對值，將該保存於記錄再生器時處理部 302 之內部記憶體 307 的核對值 B 生成輸出 Kicvb 做為輸出，並將該複寫資訊輸出 Kbit、存儲信息輸出 Kcon 及複寫資訊 (BIT) 分割成 8 組元單位並進行排他性邏輯和而將該核對值以 DES 進行暗號化後生成後之核對值 B，與被收納於黑窗 (Header) 內之核對值：ICV b 進行一致後時，用該判斷與複寫資訊輸出 Kbit、存儲信息輸出 Kcon、複寫資訊無更改。

步驟 S57 中，記錄再生器時處理部 302 之控制部 306，係在記錄再生器時處理部 302 之輸出部 308 使用中間核對值計算，中間核對值，係如圖 25 所示，將該保存於記錄再生器時處理部 302 之內部記憶體 307 的核對值 B 生成輸出 Kicvi 做為輸出，並將該核對值 (Header) 內之核對值 A、核對值 B，進行

本國際大元通商中韓專利權 (CN2004 專利 (2004) 第 117 號)

A7
B7

五、發明說明(115)

將該複寫全部之存儲信息核對值做為信息做輸出 7 已說明之 ICV 計算方法進行計算，尚有，做為初期值 $IV=0$ ，但在記錄再生器時處理部 302 之內部記憶體 307 用以保存核對值 B 生成用初期值 IV 放著，將此加以使用也可，又，生成後之中間核對值，係根據必要條件於記錄再生器 300 之記錄再生器時處理部 302 改著。

該中間核對值，係將核對值 A、核對值 B，全部之存儲信息核對值做為信息生成，將對於形成此等核對值之驗證對象的資料之驗證藉由中間核對值之核對處理進行也可，可是，本實施例中，係將做為系統全部之所有資料的非常改核對值處理，及在下載處理後後告知記錄再生器 300 做為占有之占有資料為了進行識別用以區別驗證處理差為了做為占有資料，由中間核對值而演變之不同核對值，即核對值 ICV i，及記錄再生器有核對值 ICDenv，分別根據中間核對值做輸出可生成，對於此等核對值係在後段加以說明。

記錄再生器時處理部 302 之控制部 306，係在記錄再生器時處理部 302 之輸出部 308 使用核對值 ICV i 之計算，核對值 ICV i，係如圖 25 所示，將該保存於記錄再生器時處理部 302 之內部記憶體 307 的系統著名輸出 Ksys 做為輸出，將中間核對值以 DES 進行暗號化並加以生成，最後，用以比較生成後之核對值 ICV i 及在步驟 S51 進行保存放著的 Header 內之 ICV i，在進行一致後時，即用以執行系

本國際大元通商中韓專利權 (CN2004 專利 (2004) 第 118 號)

A7
BT

五、發明說明 (120)

記錄裝置全取再生時，使記錄再生器之固有值對 ICVae 形成不一致，形成錯誤所以成為不能再生。

因此，本發明之資料處理裝置中，藉由利用限制資訊之設定，在系統可共同使用存儲信息，在記錄再生器固有值可利用之存儲信息形成可自由設定。

步驟 S63 中，記錄再生器 300 之控制部 301，係將存儲信息保存於記錄裝置 400 之外部記憶體 402。

圖 26 係顯示利用限制資訊在 0 之情形中記錄裝置內的存儲信息狀態圖。圖 27 係顯示利用限制資訊在 1 之情形中記錄裝置內的存儲信息狀態圖。圖 26 與圖 27 不同點，係將存儲信息區段資訊輸出 Kbit 及存儲信息輸出 Kcon 以記錄輸出 Kdis 被暗號化，但與保存輸出 Ktr 被暗號化。又，圖 27 與圖 26 不同點，係由中間對值部計算之被對值，在圖 26 係以系統等名稱 Kys 被暗號化，相對地在圖 27 係以記錄再生器固有之記錄再生器等名稱 Kdev 被暗號化。

再者，圖 22 之處理流程中，在步驟 S52 對被對值 A 之驗證進行失敗時，在步驟 S56 對被對值 B 之驗證進行失敗時，在步驟 S57 對被對值 C 之驗證進行失敗時，在步驟 S58 對各存儲信息區段之存儲信息區段之驗證進行失敗時，則進到步驟 S64，進行預定之錯誤顯示。

又，在步驟 S61 利用限制資訊在 0 之情形，則跳過

A7
BT

五、發明說明 (121)

步驟 S82 進到步驟 S63。

(8) 以記錄裝置固有資訊之記錄再生器之再生處理
其次以被收納於記錄裝置 400 之外部記憶體 402 的存儲信息區段之記錄再生器 300 對於再生處理加以說明。

圖 28 係用以說明使記錄再生器 300 由記錄裝置 400 讀出存儲信息，並用以利用存儲信息之程序流程圖。圖 28 中，係做為在記錄再生器 300 及記錄裝置 400 之間已使相互連接時。

步驟 S71 中，記錄再生器 300 之控制部 301，係使用記錄裝置控制部 303 由記錄裝置 400 之外部記憶體 402 讀出存儲信息。而且，記錄再生器 300 之控制部 301，係將資訊內之標章 (Header) 部分發送到記錄再生器 300 之記錄再生器暗號處理部 302。步驟 S72，係將「(7) 由記錄再生器對記錄裝置下載處理」中已說明之步驟 S52 同樣之處理，從接收集 (Header) 後之記錄再生器暗號處理部 302 之控制部 306，在記錄再生器暗號處理部 302 之暗號/譯碼化部 308 使被對值 A 計算之處理。被對值 A，係如前圖已說明之步驟 23 所示將被保存於記錄再生器暗號處理部 302 之內碼記憶體 307 的被對值 A 年或輸出 Kicva 做為輸出，將被對值 (Content ID) 及處理方針 (Usage Policy) 做為信息根據在圖 7 已說明之同樣的 ICV 計算方法被計算。

A7
BT

五、發明說明 (122)

如前圖已說明被對值 A，ICVa，係為用以驗證被對值 (Content ID) 及處理方針 (Usage Policy) 之被對值的被對值，將被保存於記錄再生器暗號處理部 302 之內碼記憶體 307 的被對值 A 生成輸出 Kicva 做為輸出，並將被對值 (Content ID) 及處理方針 (Usage Policy) 做為信息根據在圖 7 已說明之 ICV 計算方法被計算之被對值 A，將被對值 (Header) 內之被對值：ICV，進行一致後時，係將判斷被對值於記錄裝置 400 之後進到資訊，處理方針無效。

其次，步驟 S73 中，記錄再生器 300 之控制部 301，係由讀出後之集 (Header) 部分取出被對值資訊輸出 Kbit 及存儲信息輸出 Kcon，並透過記錄再生器 300 之記錄裝置控制部 303 發送到記錄裝置 400。用以將由記錄再生器 300 被發送到之區段資訊輸出 Kbit 及存儲信息輸出 Kcon 後之記錄裝置 400，係將接收後之資料在記錄裝置暗號處理部 401 之暗號/譯碼化部 406，以保存於記錄裝置暗號處理部 401 之內碼記憶體 405 的記錄裝置固有之保存輸出 Ktr 被譯碼化處理，在相互驗證時以進行共有有效之對照時間輸出 Kses 使暗號化，而且，記錄再生器 300 之控制部 301，係透過記錄再生器 300 之記錄裝置控制部 303，由記錄裝置 400 以該時間輸出 Kses 用以讀出被暗號化後之區段資訊輸出 Kbit 及存儲信息輸出 Kcon。

其次，步驟 S74 中，記錄再生器 300 之控制部

A7
BT

五、發明說明 (123)

301，係以接收後之對照時間輸出 Kses 將被暗號化後之區段資訊輸出 Kbit 及存儲信息輸出 Kcon 發送到記錄再生器 300 之記錄再生器暗號處理部 302。

以對照時間輸出 Kses 用以接收被暗號化後之區段資訊輸出 Kbit 及存儲信息輸出 Kcon 後之記錄再生器 300 之記錄再生器暗號處理部 302，係在記錄再生器暗號處理部 302 之暗號/譯碼化部 308，以該對照時間輸出 Kses 將被暗號化後之區段資訊輸出 Kbit 及存儲信息輸出 Kcon，在相互驗證時以進行共有有效之對照時間輸出 Kses 使暗號化，而且，以譯碼化後之區段資訊輸出 Kbit，在步驟 S71 將接收後放著之區段資訊使譯碼化。

再者，記錄再生器 300 之記錄再生器暗號處理部 302，係將譯碼化後之區段資訊輸出 Kbit，存儲信息輸出 Kcon 及區段資訊 BIT，在步驟 S71 讀出接收後放著之區段資訊輸出 Kbit，存儲信息輸出 Kcon 及區段資訊 BIT 並加以保持時，又，記錄再生器 300 之控制部 301，係將譯碼化後之區段資訊 BIT 由記錄再生器 300 之記錄再生器暗號處理部 302 讀出放著。

步驟 S75，係將「(7) 由記錄再生器對記錄裝置下載處理」中已說明之步驟 S56 同樣之處理，使記錄再生器暗號處理部 302 之控制部 306，由記錄裝置 400 將讀出後之區段資訊輸出 Kbit，存儲信息輸出 Kcon 及區段資訊 (BIT) 分割成 8 位元單位，並將此等全部進行譯碼化處理。其次，記錄再生器暗號處理部 302

AT
BT五、發明說明⁽¹²⁴⁾

之控制部 306，係在記錄再生時將該處理部 302 之暗號／譯碼化部 308 使核對值 B (ICVB) 計算。核對值 B，係如前面已說明所示，將被保持於記錄再生時暗號處理部 302 之內部記憶體 307 的核對值 B 生成輸出 Kicvb 做為輸出，所剩才計算後之計核性邏輯和以 DES 進行暗號化並加以生成。最後，用以比較核對值 B 及 Header 內之 ICVB，進行一致後則到達到步驟 576。

如前面已說明，核對值 B、ICVB，係為了驗證區段資訊輸出 Kbit，存儲信息輸出 Kcon，區段資訊之重寫的核對值，將被保存於記錄再生時暗號處理部 302 之內部記憶體 307 的核對值 B 生成輸出 Kicvb 做為輸出，由記錄裝置 400 所讀出後之區段資訊輸出 Kbit，存儲信息輸出 Kcon 及區段資訊 (BIT) 分割成 8 單元單位並進行計核性邏輯和將被取得值以 DES 進行暗號化並使之生成之核對值 B，與該等納於由記錄裝置 400 讀出後之資料中之 Header (Header) 內之核對值：ICVB 進行一致後時，則被訂定被保存於記錄裝置 400 後之資料的核對值輸出 Kbit，存儲信息輸出 Kcon，區段資訊無誤。

步驟 576 中，記錄再生時暗號處理部 302 之控制部 306，係在記錄再生時將該處理部 302 之暗號／譯碼化部 308 中間核對值計算，中間核對值，係如前面已說明 25 所示將被保存於記錄再生時暗號處理部 302 之內部記憶體 307 的核對值 B 生成輸出 Kicvt 做為輸出，將該核對值之 Header (Header) 內之核對值 A，核對值

本國式通用中韓語音譯 (CNS/A4 規格 (210×297 公釐)) - 127 -

AT
BT五、發明說明⁽¹²⁵⁾

B，進行保存該等之全部的存儲信息核對值做為信息根據圖 7 已說明之 ICV 計算方法進行計算。最後，做為初期值 $1V=0$ ，在記錄再生時暗號處理部 302 之內部記憶體 307 用以保存核對值生成初期值 $1V$ 啟者，再此進行使用也可。又，生成後之中間核對值，係因該值必要保持於記錄再生時 300 之記錄再生時暗號處理部 302 啟者。

再者，步驟 577 中，記錄再生時 300 之控制部 301，係由記錄裝置 400 之外部記憶體 402 被合於讀出該等之資料的輸出部由處理方針 (Output Policy) 看出利用限制資訊，使下載後之存儲信息進行判定並可利用該記錄再生時 300 (利用限制資訊為 1)，或也可利用另外同樣之記錄再生時 300 (利用限制資訊為 0)，判定之結果，利用限制資訊為 1，即下載後之存儲信息也可利用該記錄再生時 300 被判定利用限制時，則達到步驟 580，則利用限制資訊為 0，即也可利用另外同樣之記錄再生時 300 之設定時，則達到步驟 578。再者，步驟 577 之處理，係使暗號處理部 302 進行也可。

步驟 578 中，係 (7) 由記錄再生時暗號處理部 302 之暗號處理部 308 被執行利用限制時，則達到核對值 ICVT 的計算，即，記錄再生時暗號處理部 302 之控制部 306，係在記錄再生時暗號處理部 302 之暗號／譯碼化部 308 使核對值 ICVT 的計算，核對值 ICVT，係如前面已說明之圖 25 所示將被保存於記錄

本國式通用中韓語音譯 (CNS/A4 規格 (210×297 公釐)) - 128 -

AT
BT五、發明說明⁽¹²⁶⁾

再生時暗號處理部 302 之內部記憶體 307 的系統名稱輸出 Kys 做為輸出，將中間核對值以 DES 進行暗號化並加以生成。

其次，達到步驟 579，用以比較步驟 578 中之生成後之核對值 ICVT 及在步驟 571 進行保存啟者之 Header (Header) 內之 ICVT，進行一致後時，則達到步驟 582。

如前面已說明，核對值 ICVT，係為了用以驗證 ICVA，ICVB，各存儲信息重寫之核對值全部之重寫的核對值，因此，有上述之處理被生成後之核對值被保存於 Header (Header) 內之核對值：ICVT 進行一致後時，則被訂定被保存於記錄裝置 400 後之資料中，被列明 ICVA，ICVB，各存儲信息重寫之核對值全部重寫。

在步驟 577 之判定中，使進行下載之存儲信息係可利用該記錄再生時 300 之設定時，即設定資訊為 1 時，則達到步驟 580。

步驟 580 中，記錄再生時暗號處理部 302 之控制部 306，係在記錄再生時暗號處理部 302 之暗號／譯碼化部 308，使記錄再生時暗號有之核對值 ICVdev 之計算。記錄再生時暗號有之核對值 ICVdev，係如前面已說明之圖 25 所示將被保存於記錄再生時暗號處理部 302 之內部記憶體 307 的記錄再生時暗號有之記錄再生時系統名稱 Kdev 做為輸出，將中間核對值以 DES 進行暗號化並加以生成

本國式通用中韓語音譯 (CNS/A4 規格 (210×297 公釐)) - 129 -

AT
BT五、發明說明⁽¹²⁷⁾

，步驟 581 中，用以比較在步驟 580 進行計算後之記錄再生時暗號有之核對值 ICVdev 及在步驟 571 進行保存啟者之 Header 內之 ICVdev，在進行一致後時，則達到步驟 582。

如此，藉由系統名稱輸出 Kys 被署名之資料，係藉由具有與系統名稱之系統 (記錄再生時) 成功核對，即核對核對值 ICVT 形成一致時所以成為可共同利用，使用記錄再生時暗號有之核對值 ICVdev 啟者時，則記錄再生時暗號有之核對值 ICVdev 係具有固有之輸出，所以使用記錄再生時暗號有之核對值 ICVdev 被署名之資料，即，署名後，被寄附於記錄裝置之資料，係在該之記錄再生時，用以驗證該記錄裝置或再生時，使記錄再生時暗號有之核對值 ICVdev 形成一致，形成驗證所以成為不能再生。因此，藉由利用限制資訊之設定，在系統可利用保存信息，則可利用於記錄再生時暗號有之存儲信息形成可自由設定。

步驟 582 中，記錄再生時 300 之控制部 301，係在步驟 574 用以讀出進行讀出啟者之區段資訊 BIT 內之存儲信息區段資訊，並使存儲信息區段資訊是否成為暗號化對象，成為暗號化對象時，將該存儲信息區段資訊，進行記錄再生時 300 之記錄裝置控制部 303，由記錄裝置 400 之外部記憶體 402 進行讀出，並使達到記錄再生時 300 之記錄再生時暗號處理部 302，將該被讀後之記錄再生時暗號處理部 302 之控制部 306，係在記錄再生時暗號處理部 302 之暗號／譯碼化部 308 使存

本國式通用中韓語音譯 (CNS/A4 規格 (210×297 公釐)) - 130 -

五、發明說明 (128)

與新信息區，同時將存儲信息區按成列驗證對象時間在下一次步驟 S83 中使存儲信息核對值進行驗證。

步驟 S83 中，係與「7」由記錄再生器對記錄驗證之下載處理」中已說明之步驟 S58 同樣之處理，記錄再生器 300 之控制部 301，係用以取出該區段資訊 (BIT) 內之存儲信息區資訊，將存儲信息區按成列驗證對象由存儲信息核對值之狀態而進行判定，使存儲信息區按成列驗證對象，而將該存儲信息區按成列驗證 400 之外部記憶部 402 進行檢取，並發送記錄再生器 300 之記錄再生器驗證處理部 302，將該接收後之記錄再生器驗證處理部 302 之控制部 306，係在記錄再生器驗證處理部 302 之檢取/譯碼化部 308 使存儲信息中間值進行計算。

存儲信息中間值，係在步驟 S74 以譯碼化後之存儲信息區段 Kcon，將檢取輸入後之存儲信息區段以 DES 之 CBC 模式進行譯碼化，將其結果區段成 8 倍寬全部進行隨機亂數和並加以生成。

其次，記錄再生器驗證處理部 302 之控制部 306，係在記錄再生器驗證處理部 302 之檢取/譯碼化部 308 使存儲信息核對值進行計算，存儲信息核對值，係將保存於記錄再生器驗證處理部 302 之內部記憶部 307 的存儲信息核對值生成輸出 Kicrc 做為檢點，並將存儲信息中間值以 DES 進行檢點化並加以生成，而且，記錄再生器驗證處理部 302 之控制部 306，係用以比較

五、發明說明 (129)

該存儲信息核對值，及在步驟 S71 由記錄再生器 300 之控制部 301 接收後之存儲信息區段內之 ICV，並將該結果轉文到記錄再生器 300 之控制部 301，將此接收後之記錄再生器 300 之控制部 301，係在驗證進行成功後時，所以取出下次驗證對象存儲信息區段並在記錄再生器 300 之記錄再生器驗證處理部 302 從驗證，用以驗證全部存儲信息區段為止重複同樣之驗證處理，尚有，初期區段為 IV=0，在記錄再生器驗證處理部 302 之內部記憶部 307 用以保存存儲信息核對值生成用初期 ICV 數值，將此進行使用也可。又，核對後之全部的存儲信息核對值，係保持於記錄再生器 300 之記錄再生器驗證處理部 302 故軍，進而又，記錄再生器 300 之記錄再生器驗證處理部 302，係用以監視驗證對象之存儲信息區段的驗證順序，依順序錯誤，或將同一之存儲信息區段使 2 次以上驗證時，則視為進行驗證失敗。

記錄再生器 300 之控制部 301，係用以檢取該存儲信息核對值之比較結果 (未成為驗證對象時，則比較結果係全部成功)，在驗證進行成功後時，則由記錄再生器 300 之記錄再生器驗證處理部 302 取出被譯碼化後之存儲信息，而且，用以取出下次驗證對象存儲信息區段並在記錄再生器 300 之記錄再生器驗證處理部 302 從譯碼化，將全部之存儲信息區段進行譯碼化而重複進行。

五、發明說明 (130)

尚有，步驟 S83 中，記錄再生器 300 之記錄再生器驗證處理部 302，係在存儲信息核對值之驗證處理中形成不一致時，則做為驗證失敗在該時點用中止處理，而將下次存儲信息之譯碼化並不進行，又，記錄再生器 300 之記錄再生器驗證處理部 302，係用以檢取譯碼化對象之存儲信息區段的譯碼化順序，使順序有錯誤，或將同一之存儲信息區段使 2 次以上進行譯碼化時，則做為進行譯碼化失敗。

尚有，在步驟 S72 核對區 A 之驗證進行失敗時，在步驟 S75 核對值 B 驗證進行失敗時，在步驟 S79 核對值 1 CV1 驗證進行失敗時，在步驟 S81 記錄再生器固有之核對值 ICVdev 驗證進行失敗時，在步驟 S83 存儲信息區段的存儲信息核對值驗證進行失敗時，則進行步驟 S84，進行預定之圖樣顯示。

如以上所敘的說明，將存儲信息進行下載，或進行利用時，將重要的資料或存儲信息進行譯碼化故著進行譯碼化，不僅可更改驗證，為了用以譯碼化或資訊 BIT 之區段資訊輸出 Kbit，為了用以譯碼化存儲信息之存儲信息輸出 Kcon 係以記錄裝置固有之保存輸出 Kstr 因為被保存，所以單將將記錄裝置上之資料在寫的記錄裝置進行複製，也可將存儲信息不能正確地進行譯碼化，更其難而前，譬如圖 2B 之步驟 S74 中，將有在各記錄以不同保存輸出 Kstr 為用以譯碼化被驗證之資料，以別的記錄裝置保存資料不能正確譯碼化之構成。

五、發明說明 (131)

(9) 相互驗證後之檢取交換處理

本發明之資料處理裝置中特徵之一，係在上述之記錄再生器 300 及記錄裝置 400 之某處在該執行相互驗證之後，做為可記錄裝置之利用，又，無進行限制其利用無妨之點。

譬如，由於不正當複製等用以生成等存儲信息後之記憶卡等的記錄裝置，將此設定於記錄再生器為排除被利用，在記錄再生器 300 及記錄裝置 400 間執行相互驗證處理，且將形成驗證 OK 做為條件，在存儲信息 (已核對驗證) 之記錄再生器 300 及記錄裝置 400 間就可轉送。

為了用以實現上述之限制的處理，本發明之資料處理裝置中，係在記錄裝置 400 之檢取處理部 401 選擇，全部，形成構成數據預先設定後之指令列表執行，即，記錄裝置，係具有根據指令號碼將指令由順序寄存器取出並執行之指令處理構成，而 2 張顯示以該記錄裝置用以說明指令處理構成。

如圖 29 所示在具有記錄再生器驗證處理部 302 之記錄再生器 300 及具有記錄裝置驗證處理部 401 之記錄裝置 400 間，在記錄再生器 300 之控制部 301 的控制下由記錄裝置驗證部 303 對記錄裝置 400 之資訊 (含檢取存儲) 404 使指令號碼被輸出。

記錄裝置 400，係在檢取處理部 401 內之控制部

五、發明說明⁽¹³²⁾

403具有指令號碼管理部2901、指令號碼管理部2901係用以保持指令寄存部2902、由記錄再生部300用以容納對應於被輸出指令號碼的指令列、指令列、係如圖29之右所示由指令號碼0到y指令列、對指令號碼被附加有對應執行指令、指令號碼管理部2901、係由記錄再生部300用以容納被輸出指令號碼、對對應之指令由指令寄存部2902取出並加以執行。

被容納於指令寄存部2902後之指令序列、係如圖29之右所示、使有該部記憶處理序列之指令列被附加有對應於先行之指令號碼0~x、進而、使有該部記憶處理序列之指令列之後的指令號碼p~s被附加有對應譯碼、輸出交換、繼續處理指令序列1、進而、在後續之指令號碼u~y被附加有對應譯碼、輸出交換、繼續處理指令序列2。

如前圖29之記憶處理流程中已說明、使記錄裝置400被容納於記錄再生部300、則記錄再生部300之控制部301、係通過記錄裝置400、將此被後之記錄裝置400、係在記錄裝置地址管理部401之控制部403中、通過通訊部404用以接收指令、並用以被該部記憶處理部2903、即設定於未設定狀態、又、由記錄再生部300在記錄裝置400使電壓被供給後而開始、係在有電壓時被為未設定狀態進行設定方式也可。

其次、記錄再生部300之控制部301、係用以被該部記憶處理部2903、即設定於未設定狀態、此時、記

五、發明說明⁽¹³³⁾

錄裝置被入口號碼也一起發送、藉由用以發送記錄裝置被入口號碼、在記錄再生部300使電壓被供給後、時間時與被載之記錄裝置400形成可設置譯碼、及資料收發。

用以接收初期化指令後之記錄再生部300之記錄再生部被處理部302、係在記錄再生部被處理部302之控制部中、用以消除對應於記錄裝置被入口號碼之記錄被載2904、而設定於未設定狀態。

進行終了此等之初期化處理、則記錄再生部300之控制部301、係通過記錄裝置地址管理部303由指令號碼0依順序用以輸出指令號碼、記錄裝置400之指令號碼管理部2901、係由記錄再生部300用以容納被輸入指令號碼、並用以被該部0依順序被輸入、對對應之指令由指令地址2902進行取出並用以執行記錄處理等各種處理、被輸入指令號碼未依規定順序時、則被為錯誤、將指令號碼被收發為初期狀態、即進行設定並可執行指令號碼=0。

如圖29所示被容納於指令地址2902之指令序列、係用以先行被該部記憶處理部2903進行處理之指令號碼、在其後的處理被容納有譯碼、輸出交換、繼續處理之處理序列。

使用圖30、31用以說明譯碼、輸出交換、繼續處理之處理序列。

圖30係由前面圖22中已說明之記錄再生部300

五、發明說明⁽¹³⁴⁾

則記錄裝置400之存儲信息的下處處理中用以構成被執行處理的一部分、具體而言在圖22中之步驟S69~S80間被執行。

圖30中、步驟S3001、係由記錄再生部300以對照時間輸出Kses所被時鐘化後之資料(c.x、區段資訊輸出Kbit、存儲信息輸出Kcon)使記錄裝置進行接收之處理、之後、將開始的圖29所示之指令列p~s、指令列p~s被終了記錄處理指令0~k、並在圖29所示部記憶處理2903、2904使記憶處理之標記被設定後而開始、此係、使指令號碼管理部2901將指令號碼由0藉由接收依順序號碼被保證。

步驟S3002、係使記錄裝置由記錄再生部300以接收後之對照時間輸出Kses所被時鐘化後之資料(c.x、區段資訊輸出Kbit、存儲信息輸出Kcon)容納於寄存器之處理。

步驟S3003、係以對照時間輸出Kses所被時鐘化後之資料(c.x、區段資訊輸出Kbit、存儲信息輸出Kcon)由寄存器取出並用以對照時間輸出Kses用以執行譯碼之處理的步驟。

步驟S3004、係以對照時間輸出Kses所被時鐘化後之資料(c.x、區段資訊輸出Kbit、存儲信息輸出Kcon)以保存輸出Kstr用以執行繼續化之處理的步驟。

上述之處理步驟3002~3004、係包含於後面圖29已說明之指令寄存部中之指令號碼p~s處理、此

五、發明說明⁽¹³⁵⁾

等之處理、係記錄裝置400之指令號碼管理部2901中由記錄再生部300根據接收之指令號碼p~s使記錄裝置被處理部401依順序進行執行。

其次之步驟S3005、係以保存輸出Kstr將被時鐘化後之資料(c.x、區段資訊輸出Kbit、存儲信息輸出Kcon)容納於記錄裝置之外部記憶體的步驟、該步驟中、係由記錄裝置被處理部401使記錄再生部300以保存輸出Kstr用以輸出時鐘化後之資料、並在其後進行容納於記錄裝置400之外部記憶體402也可。

上述之步驟S3002~S3004、係繼續被執行不可插入的執行序列、譬如、在步驟S3003之譯碼處理終了時、由記錄再生部300即使用資料輸出指令、將其號碼輸出、係因為與被設定於指令地址2902之指令號碼p~s的依順序指令號碼不同、所以指令號碼管理部2901、係不接收輸出之執行、因此記錄裝置400中之輸出交換時將產生之譯碼資料由外部、譬如由記錄再生部300形成不可輸出、可防止輸出資料、存儲信息之不正當的輸出。

圖31係用以構成前面圖28中已說明由記錄裝置400用以輸出存儲信息並在記錄再生部300再生之存儲信息再處理中執行處理的一部分、具體而言在圖28之步驟S73中被執行之處理、圖31中、步驟S3101、係由記錄裝置400之外部記憶體402以保存輸出Kstr用以執行繼續化後之資料(c.x、區段資

五、發明說明 (136)

記錄點 Kbit、存儲信息點 Kcon 的讀出之步驟。

步驟 S3102，係由記錄裝置之記憶體以讀出後之保存點 Kstr 將被暗號化後之資料 (e.g. 高設資訊點 Kbit、存儲信息點 Kcon) 存於於存儲之步驟。該步驟中，係由記錄裝置 400 之外部記憶體 402 把記錄再生部 300 以保存點 Kstr 用以讀出被暗號化後之資料，在其後存於於記錄裝置 400 之存儲區也可。

步驟 S3103，係以保存點 Kstr 將被暗號化後之資料 (e.g. 高設資訊點 Kbit、存儲信息點 Kcon) 由存儲區取出並以保存點 Kstr 進行譯碼處理之步驟。

步驟 S3104，係以保存點 Kstr 將被暗號化後之資料 (e.g. 高設資訊點 Kbit、存儲信息點 Kcon) 以對記錄裝置 Kcon 進行暗號化處理之步驟。

上述之處理步驟 S3102~S3104，係被合於前開第 29 已說明之指令內容中之指令號碼 u-y 的處理。此等之處理，係根據裝置之指令號碼管理部 2901 中由記錄再生部 300 根據接收之指令號碼 u-y 把記錄裝置 406 依照順序進行執行。

其次之步驟 S3105，係以對時間點 Kss 將被暗號化之資料 (e.g. 高設資訊點 Kbit、存儲信息點 Kcon) 由記錄裝置進行復原到記錄再生部之處理。

上述之步驟 S3102~S3104，係根據被執行不可插入的執行序列。譬如，在步驟 S3103 之翻譯處理時點，由記錄再生部 300 即要有資料讀出指令，

五、發明說明 (137)

將其讀出指令，係因為其係設定於指令地址 2902 之指令號碼 u-y 的順序而指令號碼不同，所以指令號碼管理部 2901，係不接收讀出之執行。因此記錄裝置 400 中之編碼交換將產生之譯碼資料由外部，譬如由記錄再生部 300 形成不可讀出，可防止讀出資料、存儲信息之不正當的讀出。

尚有，圖 30、31 所示之處理，係藉由編碼交換被譯碼，暗號化對象，顯示有高設資訊點 Kbit、存儲信息點 Kcon 之處，但被容納於此等之圖 29 所示之指令中而存於 2902 後之指令序列。係根據存儲信息與由編碼交換含有譯碼，暗號化處理也可，藉由編碼交換被譯碼，暗號化對象係不限於上述之例。

以上，對於本發明之資料處理裝置中相互關係後的編碼交換處理做了說明。如此，本發明之資料處理裝置中之編碼交換處理，係在記錄再生部及記錄裝置間而在移了記錄裝置後亦可執行，進而，由編碼交換處理中之譯碼資料的外部即可防止存取的情況，所以使存儲信息、編碼資料之高度之安全性被確保。

(10) 複數之存儲信息格式，及對應於各格式的下載及再生處理

上述之實施例，係假定裝置 30 所稱號碼 500 或號碼 600 中之資料格式對應於圖 4 所示 1 種的情況做了說明。可是，係將 500 或號碼 600 中之資料格式，

五、發明說明 (138)

係不限於於上述圖 4 所示之格式，被存儲信息有新增之情形，有刪除資料之情形，遊戲等之格式的情形等，係根據存儲信息以採用資料格式異樣性。以下，對於複數之不同的資料格式，及對應於各格式之記錄裝置之下載處理及由記錄裝置之再生處理加以說明。

圖 32~35 係表示 4 種不同的資料格式。在各圖之左側，係表示圖 30 所示號碼 500 或號碼 600 中之資料格式。又在各圖之右側係顯示被存於於記錄裝置 400 之外部記憶體 402 時之資料格式。首先，用以說明圖 32~35 所示資料格式之概略。之後，對於各格式中之各資料的內容，及各格式中之資料的差異加以說明。

圖 32，係格式形態 0。在上述之說明中係將例示之形態 0 及共同形態。該格式形態 0 之特徵，係將資料全體分割成任意大小之 N 個之資料區段，即分割成區段 1~區段 N，對於各區段任意進行暗號化，可構成暗號化區段及非暗號化區段。即，使在平常文或可構成資料之點、區段之暗號化，係藉由存儲信息點 Kcon 來執行，存儲信息點 Kcon，係在媒體上藉由配送點 Kdis 被暗號化。在記錄裝置中之保存時，係藉由被容納於記錄裝置之內部記憶體的保存點 Kstr 被暗號化。對於高設資訊點 Kbit 也在媒體上藉由配送點 Kdis 被暗號化。在記錄裝置中之保存時，係藉由被容納於記錄裝置之內部記憶體後之保存點 Kstr 被暗號化。此等之點之交換，係根據前開之「(9)」相互關係後的點之交換處理，中說明之處理被執行。

五、發明說明 (139)

圖 33，係格式形態 1。該格式形態 1，係將格式形態 0 同樣，將資料全體分割成 N 個之資料區段，即分割成區段 1~區段 N，但將 N 個之區段之大小做為均等大小之點係與前開格式形態 0 不同。藉由存儲信息點 Kcon 使區段之暗號化處理係與前開之格式形態 0 同樣。之後，在媒體上藉由配送點 Kdis 被暗號化。在記錄裝置中之保存時係藉由被容納於記錄裝置之內部記憶體後之保存點 Kstr 被暗號化。存儲信息點 Kcon 及高設資訊點 Kbit 構成也與上述格式形態 0 同樣。格式形態 1，係與格式形態 0 不同，做為固定性的區段構成，使各區段之資料長度等之構成資料被暗號化，所以此格式形態 0 成為可減少區段資訊之記錄體大小。

圖 33 之構成例，係將各區段藉由暗號化部分及非暗號化部分 (平常文) 之 1 個進行構成。如此區段之長度，係構成若有規則性，則在譯碼處理時可區段長度，形成不應用以區段區段構成所以成為可有效譯碼，暗號化處理。尚有，在格式 1 中，用以構成各區段之部分，即暗號化部分，非暗號化 (平常文) 部分，係在各部分做為相對對象可定義的構成。也要對於零件之區段時，係關於其區段保存點信息核對 I C V I 被設定。

圖 34，係格式形態 2。該格式形態 2 之特徵，係用大小之 N 個之資料區段，即被分割成區段 1~區段 N，對於各區段，分別以個別之區段點 Kdis 被暗號化。各區段點 Kdis，係在媒體上藉由配送點 Kdis 被暗號化。在

AT
BT五、發明說明⁽¹⁴⁰⁾

記錄裝置中之保存時，係藉由容納於記錄裝置之內部記憶體後之保存端點 Kstr 被暗號化。對於寫入資訊端點 Kbit 也在寫入藉由配速端點 Kdis 被暗號化。在記錄裝置中之保存時，係藉由容納於記錄裝置之內部記憶體後之保存端點 Kstr 被暗號化。

圖 35，係格式形態 3，該格式形態 3 之特徵，係將格式形態 2 同樣，與樣大小之 N 個之資料區段，即被分割成區段 1 ~ 區段 N，對於各區段，分別以個別之區段端點 Kbic 被暗號化，並用，不使用存儲信息點，各區段端點 Kbic 之暗號化，係在媒體上藉由配速端點 Kdis 被暗號化。在記錄裝置上係藉由存儲點 Kstr 被暗號化之點，存儲信息點 Kcon，係在媒體上，裝置上，皆不存在。寫入資訊端點 Kbit 係在媒體上藉由配速端點 Kdis 被暗號化。在記錄裝置中之保存時，係藉由容納於記錄裝置之內部記憶體後之保存端點 Kstr 被暗號化。

其次，對於上述格式形態 0 ~ 3 之資料內容加以說明，資料係如前述之說明，並分成廣播資訊及存儲信息點 2 資料，廣播資訊係含有存儲信息點識別子，處理方針，核對值 A、B，該核對值，區段資訊點，存儲信息點，區段資訊。

處理方針，係存儲信息之資料長，廣播長，格式形態（以下說明之格式形態 0 ~ 3），資訊用格式，區段資料等之存儲信息點，對於該之存儲信息之記錄裝置的下載，如再生之讀的說明，使存儲信息用決定在記錄再生裝置

本領域之普通技術者應能容易地理解本發明之技術特徵。圖 35 係格式形態 3 之說明圖。

AT
BT五、發明說明⁽¹⁴¹⁾

有是否可利用之應記的局部性暗記，並用，存儲信息之複製，有關於暗記之許可標誌，並用，存儲信息暗記化算法，模式等，用以容納有關存儲信息之各種的利用限制資訊及處理資訊。

核對值 A：ICVa，係對區段資訊點，處理方針之核對值，譬如，藉由前述圖 23 說明之方法被生成。

區段資訊點 Kbit，係為了用以暗記化區段資訊點之端點，如前述之說明，在媒體上藉由配速端點 Kdis 被暗號化，在記錄裝置中之保存時，藉由容納於記錄裝置之內部記憶體後之保存端點 Kstr 被暗號化。

存儲信息點 Kcon，係僅用於存儲信息之端點，格式形態 0、1，係與區段資訊點 Kbit 同樣在媒體上藉由配速端點 Kdis 被暗號化，在記錄裝置中之保存時，係藉由容納於記錄裝置之內部記憶體後之保存端點 Kstr 被暗號化。尚有，在格式形態 2，存儲信息點 Kcon，係被構成於存儲信息各區段在區段端點 Kbic 之暗號化後被利用，又，該格式形態 3 中，存儲信息點 Kcon 係不存在。

區段資訊，係用以記錄個別之區段資訊的圖表，區段之大小，對於該區段暗號化之標誌，即顯示各區段是否形成核對對象（ICV）容納資訊，區段形成核對對象時，則形成區段之核對值（ICV）（區段之核對值）在圖表中被定義並被容納。該區段資訊，係藉由區段資訊端點 Kbit 被暗號化。

尚有，區段之核對值，用存儲信息核對值 ICV1，

本領域之普通技術者應能容易地理解本發明之技術特徵。圖 36 係格式形態 3 之說明圖。

AT
BT五、發明說明⁽¹⁴²⁾

係將區段被暗號化時，將平常文（源碼文）主體以 8 組元單位進行暗號化處理和之值以被容納於記錄再生器 300 之內部記憶體 307 後之存儲信息點對值生成端點 Kbic 做為暗號化之值被生成。又，區段未被暗號化時，則將廣播資訊（平常文）之全體以 8 組元單位輸入於圖 36 所示寫入資訊點生成圖表（DRS-CBC-MAC，將存儲信息核對值生成端點 Kbic 做為取得之值被生成。圖 36 係顯示用以生成存儲信息點之核對值 ICV1 之構成例。信息 M 之各自係用以編碼源碼文資料或平常文資料之各 8 組元。

尚有，在格式形態 1 中，係在區段內之零件中至少 1 個內核對值 ICV1 之對象資料，即係核對零件時，則有關區段被暗號化後之存儲信息點對值 ICV1，區段 1 中之零件 j 之核對值 P-ICV1j，係使零件 j 被暗號化時，將平常文（源碼文）主體以 8 組元單位進行暗號化處理和之值以存儲信息核對值生成端點 Kbic 做為取得之值被生成。又，使零件 j 未被暗號化時，將零件 j 之區段資料（平常文）之全體以 8 組元單位輸入於圖 36 所示寫入資訊點生成圖表（DRS-CBC-MAC，將存儲信息核對值生成端點 Kbic 做為取得之值被生成。

進而，在 1 個區段內，內顯示有核對對象（ICV 標記 = subject of ICV）之零件，即係核對零件時 1 個存在時，則以上述方法生成之核對值 P-ICV1 並被暗號化後之核對值 ICV1，又，在 1 個區段內，內顯示有核對對象（

本領域之普通技術者應能容易地理解本發明之技術特徵。圖 37 係格式形態 3 之說明圖。

AT
BT五、發明說明⁽¹⁴³⁾

ICV 標記 = subject of ICV）之零件係被暗號化時，則將該段之零件核對值 P-ICV1j 以連接於零件號碼順序之資料做為對象以 8 組元單位輸入於圖 37 所示寫入資訊點生成圖表（DRS-CBC-MAC，將存儲信息核對值生成端點 Kbic 做為取得之值被生成。圖 37 係顯示用以生成存儲信息點之核對值 ICV1 之構成例。尚有，在格式形態 2、3 中，區段之核對值 ICV1 係未被定義。

核對值 B：ICVB，係對區段資訊點，存儲信息點，區段資訊點之核對值，譬如，在圖 24 藉由說明之方法被生成。

核對值 ICV1，係前述之核對值 A：ICVa，核對值 B：ICVB，進而被包含於存儲信息之核對對象的各區段核對值 ICV1 之核對對象，如前述圖 25 之說明核對值 A：ICVa 等之核對值在被生成中間被核對值適用系統等名稱 Ksys 藉由用以執行暗號化處理被生成。

尚有，在格式形態 2、3 中，核對值 ICV1，係在前述之核對值 A：ICVa，核對值 B：ICVB 存儲信息資料，即由區段 1 之區段端點 Kbic 到最後區段 j 止由用以連結存儲信息資料之零件在生成中間被核對值適用系統等名稱 Ksys 並藉由用以執行暗號化處理被生成。圖 38 係顯示用以生成格式形態 2、3 中之核對值 ICV1 之構成例。

本領域之普通技術者應能容易地理解本發明之技術特徵。圖 38 係格式形態 3 之說明圖。

A7
B7

五、發明說明(144)

則有相對值 ICVdew，係使前述之局部化標記被設定於 1 時，即，使存儲信息顯示在記錄再生部固有可利用時，被置換成對應值 ICVt 之相對值，格式形態 0、1 時，係該值之相對值 A：ICVa，相對值 B：ICVb，進而對被合於形成存儲信息之相對對象的各個相對值 ICVt 全體被轉換成相對值。其理由，如附圖 25，或圖 38 之說明由相對值 A：ICVa 等之各個相對值在生成中間相對值選用記錄再生部名稱 Kdev 藉由以執行邏輯化處理被生成。

其次在格式形態 0~3 各自由中記錄再生部 300 對記錄裝置 400 之存儲信息的下載處理，及對於記錄再生部 300 中由記錄裝置 400 之再生處理使用圖 39~44 之流程圖加以說明。

首先，對於格式形態 0、1 中之存儲信息的下載處理使用圖 39 加以說明。

圖 39 所示處理，係當加在記錄再生部 300 藉由以記錄裝置 400 部被讀取時，步驟 S101，係在記錄再生部及記錄裝置間之認證處理步驟，係將前面說明之圖 2 的認證處理流程圖被執行。

從步驟 S101 之認證處理終了，並從認證標記被設定，則記錄再生部 300，係在步驟 S102 中，藉由由用以寄存存儲信息資料之媒體 500，透過讀取部 304 用以讀出根據預定之格式之資料，或使透過讀取部 305 由通訊裝置 600 用以讀取根據預定之格式之存儲信息，並

本國際專利申請案係根據 ICN:541 條第 (2)(3) 項公佈 - 147 -

A7
B7

五、發明說明(145)

使記錄再生部 300 之控制部 301，將資料內之標管 (Header) 部分讀取於記錄再生部 300 之記錄再生部號碼處理部 302。

接著，步驟 S103 中，使記錄再生部號碼處理部 302 之控制部 306 在記錄再生部號碼處理部 302 之暗號／譯碼化部 308 被相對值 A 進行計算，相對值 A，係如圖 23 所示，將該保存於記錄再生部號碼處理部 302 之內部記憶體 307 的相對值 A 生成編號 Kicva 做為輸出，並將該相對資訊 (Content ID) 及處理方針 (Usage Policy) 做為信息根據使用圖 7 之說明 (ICV 計算方法被計算。其次，步驟 S104 中，所以比較相對值 A 及被寄附於標管 (Header) 內之相對值 ICVa，在進行一致時期則進到步驟 S105。

如前面說明之相對值 A、ICVa，係為了用以驗證該相對資訊，處理方針之更改的相對值，將該保存於記錄再生部號碼處理部 302 之內部記憶體 307 的相對值 A 生成編號 Kicva 做為輸出，將該相對資訊 (Content ID) 及處理方針 (Usage Policy) 做為信息，譬如使根據 ICV 計算方法被計算之相對值 A，與被寄附於標管 (Header) 內的相對值 ICVa 進行一致時，則被判斷為相對資訊，處理方針無誤。

其次，步驟 S105 中，記錄再生部號碼處理部 302 之控制部 306，係使配定編號 Kdis 之取出或生成在記錄再生部號碼處理部 302 之暗號／譯碼化部 308

本國際專利申請案係根據 ICN:541 條第 (2)(3) 項公佈 - 148 -

A7
B7

五、發明說明(146)

進行，則配定編號 Kdis 之生成方法，係與前面說明之圖 22 的步驟 S53 同樣，譬如使用配定編號 B 之主編號 Kdis 進行。

其次步驟 S106 中，記錄再生部號碼處理部 302 之控制部 306，係使用記錄再生部號碼處理部 302 之暗號／譯碼化部 308，並使用生成後之配定編號 Kdis，透過讀取部 304 由讀取後之媒體 500，或透過通訊部 305 由通訊裝置 600 進行存儲等將讀取後之資料的對象部之區段資訊編號 Kbit 及存儲信息編號 Kcon 的譯碼化處理。

進而，步驟 S107 中，記錄再生部號碼處理部 302 之控制部 306，係在記錄再生部號碼處理部 302 之暗號／譯碼化部 308 中，以譯碼化後之區段資訊編號 Kbit 用以譯碼化區段資訊。

進而，步驟 S108 中，記錄再生部號碼處理部 302 之控制部 306，係由區段資訊編號 Kbit，存儲信息編號 Kcon 及區段資訊 (BIT)，用以生成相對值 B (ICVb)，相對值 B，係如圖 24 所示，將該保存於記錄再生部號碼處理部 302 之內部記憶體 307 的相對值 B 生成編號 Kicb 做為輸出，將由區段資訊編號 Kbit、存儲信息編號 Kcon 及區段資訊 (BIT) 所構成之譯碼化邏輯和以 DES 進行邏輯化並加以生成。其次，步驟 S109 中，用以比較相對值 B 及標管 (Header) 內之 ICVb，進行一致時期則進到步驟 S110。

本國際專利申請案係根據 ICN:541 條第 (2)(3) 項公佈 - 149 -

A7
B7

五、發明說明(147)

如前面已說明，相對值 B、ICVb，係為了用以驗證區段資訊編號 Kbit，存儲信息編號 Kcon，區段資訊的更改之相對值，將該保存於記錄再生部號碼處理部 302 之內部記憶體 307 的相對值 B 生成編號 Kicb 做為輸出，將區段資訊編號 Kbit、存儲信息編號 Kcon 及區段資訊 (BIT) 分割成 8 組元單位並進行即性邏輯和將該取得之值以 DES 進行邏輯化並生成後之相對值 B，將該寄附於標管 (Header) 內之相對值 ICVb 一致時，則被判斷為區段資訊編號 Kbit、存儲信息編號 Kcon、區段資訊無誤。

步驟 S110 中，記錄再生部號碼處理部 302 之控制部 306，係在記錄再生部號碼處理部 302 之暗號／譯碼化部 308 被中相對值 B 之計算，中間相對值，係如圖 25 所示，將該保存於記錄再生部號碼處理部 302 之內部記憶體 307 的相對值 B 生成編號 Kicv 做為輸出，將進行驗證後之 Header 內之相對值 A，相對值 B，進行保持及寄之全部的存儲信息相對值再將信息在圖 7 其他被中間相對值之 ICV 計算方法進行計算，再者，生成後之中間相對值，係根據必須保持於記錄再生部 300 之記錄再生部號碼處理部 302 放著。

其次，步驟 S111 中，記錄再生部號碼處理部 302 之控制部 306，在記錄再生部號碼處理部 302 之暗號／譯碼化部 308 被相對值 ICVt 之計算，將該相對值 ICVt，係如圖 26 所示，將該保存於記錄

本國際專利申請案係根據 ICN:541 條第 (2)(3) 項公佈 - 150 -

AT
ED

五、發明說明 (148)

將生器暗號生成部 302 之內部記憶體 307 的系統署名輸出 Kys，微寫輸出，將中間核對值以 DES 進行暗號化並加以生成，其次，在步驟 S112 中，用以比較生成後之總核對值 1Cvt 及集管 (Header) 內之 1Cvt，進行一致後時，則進到步驟 S113。

如前面圖 4 中之設想，總核對值 I CV t，係為了用以核對 I CV a、I CV b，各存儲信息區段之核對值全部之累加的核對值。因此，藉由上述之處理使被生成後之總核對值與被容納於表首 (Header) 內後之核對值：I CV t 進行一致後時，則被判定 I CV a、I CV b，各存儲信息區段之核對值全部無誤。

保存價值區段形成最終對象時，則在步驟 114 中，將該套之存儲信息區段，使用記錄再生部 300 之讀取部 304 由磁碟 500 讀出，使用記錄再生部 300 之送信部 305 由通訊線路 600 進行發送，並發送到記錄再生部 302 之記錄再生器唯讀處理部 302，將此接收後之記錄再生器唯讀處理部 302 之輸出部 306，係在記錄再生器系統號碼部 302 之階層部 308 保存存儲信息校對值 I C V i 進行計算。

存儲信息值 I C V I'，係如前面說明使區段被碎化後時，以存儲信息編號 Kcon，將被輸入後之存儲信息區段以 D E S 之 C B C 模式行碎化，並將其結果以 8 組元單位進行階級性邏輯和將生成後之存儲信息中間值以被收納於記錄再生部 300 之內即記憶體 307 後之存儲

AT
RT

五、聲明說明 (149)

信息核對值生成函數 Kicvc 進行增強並加以生成。又，使區段未被暗號化時，則將資料（平常文）全體以 8 組元素位輸入於圖 3-6 所示之資訊核對值生成函數（DES-CBC-MAC），將存儲信息核對值生成函數 Kicvc 作為輸出值，輸出暗碼值並生成。

其次在步驟 S115 中，記錄再生應酬處理部 302 之控制部 306，係用以比較再生應酬信息表對照，及在步驟 S102 中記錄再生應酬 300 之控制部 301 接收之存儲信息區段內的 1CV，並將其結果轉交到記錄再生應酬 300 之控制部 301，將比較接收之記錄再生應酬 300 之控制部 301，係在輸出進行成功時，用以取出下次之輸出對象存儲信息區段在記錄再生應酬 300 之記錄再生應酬處理部 302 來驗證，用以將該接收之存儲信息區段重新校正處理之輸出信息表（步驟 S116）。

尚有，步驟 S 104，步驟 S 109，步驟 S 112，步驟 S 115 之其中之一中，未取得模範個之一致時則做為錯誤進行下載處理終了。

其次，步驟 S117 中記錄再生步 300 之記錄再生
導嘴噴流處理部 302，係以步驟 S106 所導出之化生
處理資訊輸出 Kbit 及存儲資訊輸出 Kcom，在記錄再生後之噴
流處理部 302 之噴嘴 / 導嘴化部 308，在相互距離時以
進行共有致密之對話時間輸出 Ksee 使進行噴嘴化，記錄再
生步 300 之控制部 301，係以該對話時間輸出 Ksee 將進
行噴嘴化後之導嘴資訊輸出 Kbit 及存儲資訊輸出 Kcom 由

N
87

五、發明說明 (150)

錄再生番 300 之記錄再生番暗號處理部 302 讀出。並將此等資料通過記錄再生番 300 之記錄與置換制御番 303 發送到記錄裝置 400。

其次，步驟 S118 中，由記錄器 300 用以接收被設定值來之資訊裝置識別碼 Kbit 及存儲信息庫 Kcon 後之記錄號碼 300，係根據該之資料在記錄號碼表 401 中之時間 T 之號碼 T 及 406，在相互信息庫中以進行共有號碼之對照號碼 Kbit 進行搜尋，以儲存於記錄號碼表處理部 401 中之部記憶庫 405 的記錄號碼及有之存儲號碼 Kbit 程度之號碼化，記錄器生部 300 之控制部 301，係透過記錄器生部 300 保存之記錄號碼表控制部 303，由記錄號碼表 401 以存儲信息庫 Kcon 出，以配定號碼 Kcon 之號碼化後之資訊裝置識別碼 Kbit 及存儲信息庫 Kcon 之號碼化之資訊裝置識別碼 Kbit 之號碼化。

其次，依據 S1119 中「記錄再生器 300 之控制部 301，係由資料之業者所處理方式」(Usage Policy) 取出利用限制資訊，使下載之內容信息進行判定是否可利用該記錄再生器 300。該判定，係顯示被設定於局部化資訊(利用限制資訊)=1 時，則使進行下載後之存儲信息也可利用該記錄再生器 300，而被設定於局部化資訊(利用限制資訊)=0 時，則使進行下載後之存儲信息也可利用別的其他之記錄再生器 300。判定之結果，在局部化資訊(利用限制資訊)=1 時，則將存儲信息

A2
R2

五、發明說明 (151)

步驟 S120 中，記錄再生部 300 之控制部 301 係將記錄再生部 300 之核對值在記錄再生部 300 之記錄再生部增設處理部 302 使用進行計算。記錄再生部 300 之核對部，係依照步驟 2 所示在保存於記錄再生部增設處理部 302 之內部記憶體 307 之記錄再生部所讀出之記錄再生部寄售值 Xdev 係為輸出。在步驟 S110 將生成後之中間核對值以 DES 進行變換化加如以生成，被計算後之記錄再生部 300 之核對部 ICVdev，係取代核對值 ICV T 值上。

步驟 S110 中, 記錄再生器 300 之控制部 301, 係將記錄再生器面有之核對值在記錄再生器 300 之記錄再生器號碼地址部 302 處進行存貯。記錄再生器面有之核對值, 係如圖 25 所示在裝入於記錄再生器號碼地址部 302 之內即記錄部 307 的記錄再生器面有之記錄再生器型號名 Xder 做為核對值。在步驟 S110 將生成後之中間核對值以 D E S 進行雜化並加以生成, 該計算後之記錄再生器面有之核對值 I C Vder, 係取代總核對值 I C V T 被存上。

如前圖說明，系統標名號 Ksys，係在記號系統為下列上列標名號 I CV 使用之系統標名號 Ksys，又，記錄標名號 Kdsv，在右記號再生器中，使用該標名號為下列上列標名號 I CV 使用之記錄標名號 Kdsv，即，藉由系統標名號 Ksys 恆等名後之資料，而藉由具有同標名號 Kdsv 之記錄標名號 Kdsv (記錄標名號) 使用生成，所以，使記錄標名號 I CV 形成一致，所以成爲其共同可利用，但使用記錄標名號 Kdsv 標名號之資料，而記錄標名號 Kdsv 標名號係具有其記錄標名號 Kdsv 標名號，所以使用記錄標名號 Kdsv 標名號 Kdsv 並標等名後之資料，即，「標名號」並，而於記錄標名號之資料，係在右記號再生器中，用以與該系統標名號 Kdsv 再生，使記錄標名號 Kdsv 之標名號 I CV 形成一致，成爲與圖用所以形成不能再生，本發明之資料處理裝置，係藉由該系統標名號 Ksys 與記錄標名號 Kdsv

五、發明說明(152)

使用存儲信息，將可利用的記錄再生器固有之存儲信息以自由可變定。

其次，在步驟 S121 中，記錄再生部 300 之控制部 301，係在記錄再生器端讀取部 302 讀取納資料格式之形成被執行。如前面之說明，格式形態係有 0~3 種之各種形態，被設定為其管中之處理方針（參考圖 5）中，根據該設定，依前面說明之格式 32~35 的範圍等納格式用以形成資料，該圖 39 所示處理流程格式 0、1 之其中之一，所以在圖 32、33 之其中之一之格式被形成。

步驟 S121 中使納資料格式之形成進行終了，則步驟 S122 中，記錄再生部 300 之控制部 301，係將存儲信息保存於記錄裝置 400 之外部記憶部 402。

以上，依格式形態 0、1 中之存儲信息資料之下載處理的態樣。

其次，對於格式形態 2 中之存儲信息資料的下載處理使用圖 40 加以說明，與上述之格式形態 0、1 之下載處理將不同點為中心加以說明。

步驟 S101~S109，係與上述之格式 0、1 之下載處理同樣所以省略說明。

格式形態 2，係如前面之說明使存儲信息被對照 ICV1 未被定應，所以在該說明中，未將存儲信息被對照 ICV1，格式形態 2 中之中間被對照，係如圖 38 所示由被對照 A、被對照 B，及第 1 區段之前部資料（區

五、發明說明(153)

段 1 之區段被對照) 到最後區段為止被讀用以連帶存儲信息資料全區後之資料在該生成中與被對照適用系統等名稱 Ksys 藉由用以執行暗號化處理被生成。

因此，格式形態 2 之下載處理中，係用以讀出步驟 S151 中之存儲信息資料，在步驟 S152 中，根據被對照 A、被對照 B 及讀出後之存儲信息資料用以執行中間被對照之生成，尙有，存儲信息資料係暗號化時，也不進行譯碼處理。

在格式形態 2，係如前述之格式形態 0、1 之處理不進行存儲信息資料之譯碼，存儲信息被對照之相對處理，所以係為適宜可處理。

步驟 S111 以下之處理，係與格式形態 0、1 中之處理同樣所以省略說明。

以上，依格式形態 2 中之存儲信息資料的下載處理之態樣，如上述之格式形態 2 之下載處理，係如格式形態 0、1 之處理不進行存儲信息資料之譯碼，存儲信息被對照之相對處理，所以係為適宜可處理，按需要等時處理適用於資料處理之格式。

其次，對於格式形態 3 中之存儲信息資料的下載處理使用圖 41 加以說明，與上述之格式形態 0、1、2 之下載處理將不同點為中心加以說明。

步驟 S101~S105，係與上述之格式形態 0、1、2 之下載處理同樣所以省略說明。

格式形態 3，係基本上與格式形態 2 中之處理共同之

五、發明說明(154)

部分較多，依格式形態 3 係未具有存儲信息態樣，又，依區段被對照 Kbic 在記錄裝置中係以保存被對照 Kstr 被暗號化被對照之點與格式形態 2 不同。

格式形態 3 之下載處理中與格式形態 2 將不同之點為中心加以說明，格式形態 3，係步驟 S105 之下步驟的步驟 S161 中，進行區段資訊被對照之譯碼，使記錄再生器端讀取部 302 之暗號/譯碼部 306，使用記錄再生器端讀取部 302 之暗號/譯碼部 308，至步驟 S105 使用生成後之配定被對照 Kdis，從區段讀取部 304 由接收後之讀取 500，或透過通訊部 305 由通訊裝置 600 進行被對照於接收後之資料的區段被對照 Kbic 的譯碼化處理。在格式形態 3，係在資料中因為不存在存儲信息態樣 Kcon，所以存儲信息態樣 Kcon 之譯碼化處理係不被執行。

其次之步驟 S107，係在步驟 S161 使用譯碼後之區段資訊被對照 Kbic 以使區段資訊之譯碼被執行，進而，在步驟 S162 中，記錄再生器端讀取部 302 之控制部 306，係由區段資訊被對照 Kbic，及區段資訊 (BIT)，用以生成被對照 B (ICVb)，被對照 B，係將保存於記錄再生器端讀取部 302 之內部記錄部 307 的被對照 B 生成被對照 Kicb 係為被對照，將由區段資訊被對照 Kbic，及區段資訊 (BIT) 所構成被對照性態樣和以 DES 進行暗號化並加以生成。其次，在步驟 S109 中，用以比較被對照 B 及區段 (Header) 內之 ICVb，

五、發明說明(155)

進行一致後則達到步驟 S151。

在格式形態 3，被對照 B、ICVb，係為用以驗證區段資訊被對照 Kbic，區段資訊之更改係為被對照被對照功能，係生成後之被對照 B，被對照被對照 (Header) 內之被對照 B，ICVb 進行一致後時，則所判定區段資訊被對照 Kbic，區段資訊被對照更改。

步驟 S151~S112，係與格式形態 2 之處理同樣所以省略說明。

在步驟 S163，係以步驟 S151 再被合於讀出後之存儲信息資料的區段被對照 Kbic 在步驟 S105 藉由生成後之配定被對照 Kdis 進行譯碼。

其次步驟 S164，係使記錄再生部 300 之記錄再生器端讀取部 302，將在步驟 S161 進行譯碼後之區段資訊被對照 Kbic，及在步驟 S163 進行譯碼後之區段被對照 Kbic，在記錄再生器端讀取部 302 之暗號/譯碼部 308，在相互被對照以進行具有被對照的對照性態樣 Kkes 使暗號化，記錄再生部 300 之控制部 301，係以對照時間被對照 Kses 將暗號化後之區段資訊被對照 Kbic 及區段資訊被對照 Kkes 由記錄再生部 300 之記錄再生器端讀取部 302 讀出，並將此等之資料透過通訊部 300 之記錄裝置控制部 303 傳送到記錄裝置 400。

其次，步驟 S165 中，由記錄再生部 300 將被對照之區段資訊被對照 Kbic 及區段被對照 Kkes 進行接收後之記錄裝置 400，係將接收後之資料在該生成中與被對照適用系統等名稱 Ksys 藉由用以執行暗號化處理被生成。

五、發明說明 (156)

即 401 之增號／譯碼化部 406，在相互延時時以進行共有放著對照時間點 Ktes 並譯碼化，以保存於記錄裝置時號處理部 401 之內部記憶體 405 的記錄裝置間有之保存點 Kstr 並再增號化，記錄再生部 300 之控制部 301，係透過記錄再生部 300 之記錄裝置控制部 303，由記錄裝置 400 以保存點 Kstr 用以讀出被再增號化後之區段資訊點 Kbit 及區段資訊點 Kbic，即，當對，以配適點 Kbit 將被增號化後之區段資訊點 Kbit 及區段資訊點 Kbic 以保存點 Kstr 進行資料再增號化後之區段資訊點 Kbit 及區段資訊點 Kbic。

以下之步驟 S119 ~ S122，係用前述之格式形態 0、1、2 同樣所以省略說明。

以上，係格式形態 3 中之存儲信息資料之下載處理之態樣。如上所述格式形態 3 之下載處理，係以格式形態 2 同樣，不進行存儲信息資料之讀取，存儲信息資料之讀取處理，所以成內品運送可成，並可求音樂等資料處理適用於資料運送之格式，又，藉由區段資訊點 Kbit 用以處理時使存儲信息被範圍被增號化，所以比較起格式形態 2，形成更高度的安全性。

其次，對於在格式形態 0 ~ 3 各組之記錄再生部 300 中由記錄裝置 400 之再生處理使用圖 42 ~ 45 之流程圖加以說明。

首先，對於格式形態 0 中之存儲信息的再生處理使用圖 42 加以說明。

本圖格式使用中國國家標準 (GB2444 規格 (219 ~ 259 公量)) - 150 -

五、發明說明 (157)

步驟 S201，係記錄再生部及記錄裝置間之認證處理步驟，根據圖面說明之圖 20 的認證處理流程圖執行。

使步驟 S201 之認證處理進行終了，並使延時被設定，則記錄再生部 300，係在步驟 S202 中，由記錄裝置 400 根據預定之格式用以讀出資料之美音，並發送到記錄再生部 300 之記錄再生部增號處理部 302。

其次，步驟 S203 中，使記錄再生部增號處理部 302 之控制部 306，在記錄再生部增號處理部 302 之增號／譯碼化部 308 求取對值 A 進行計算，求取對值 A，係如圖面說明之圖 23 所示，將保存於記錄再生部增號處理部 302 之內部記憶體 307 的核對值 A 生成點 Kicra 取為處理，並將識別資訊 (Content ID) 及處理方針 (Usse Policy) 作為信息計算。其次，在步驟 S204 中，用以比較被計算後之核對值 A 與被寄納於集管 (Header) 內之核對值：ICV a，進行一致時則進到步驟 S205。

核對值 A、ICV a，係為了用以驗證識別資訊，處理方針之更改的核對值，使計算其後之核對值 A，與被寄納於集管 (Header) 內之核對值：ICV a 進行一致後時，則被判斷並寄納於記錄裝置 400 後之識別資訊，處理方針無更改。

其次，步驟 S205 中，記錄再生部 300 之控制部

本圖格式使用中國國家標準 (GB2444 規格 (219 ~ 259 公量)) - 150 -

五、發明說明 (158)

301，係由讀出後之集管以記錄裝置間有之保存點 Kstr 取出被增號化後之區段資訊點 Kbit 及存儲信息點 Kcon，並透過記錄再生部 300 之記錄裝置控制部 303 發送到記錄裝置 400。

由記錄再生部 300 將被發送到而之區段資訊點 Kbit 及存儲信息點 Kcon 被接收後之記錄裝置 400，係將接收後之資料在記錄裝置增號處理部 401 之增號／譯碼化部 408，以保存於記錄裝置增號處理部 401 之內部記憶體 405 的記錄裝置間有之保存點 Kstr 被增號化處理，在相互延時時以進行共有放著的對照時間點 Ktes 被再增號化，該處理，係如在前述之 (9) 相互延時之論述交換處理的欄之詳細說明。

步驟 S206，係記錄再生部 300 之控制部 301，透過記錄再生部 300 之記錄裝置控制部 303，由記錄裝置 400 以對照時間點 Ktes 用以接收被再增號化後之區段資訊點 Kbit 及存儲信息點 Kcon。

其次，步驟 S207 中，記錄再生部 300 之控制部 301，係以進行接收後之對照時間點 Ktes 將被再增號化後之區段資訊點 Kbit 及存儲信息點 Kcon 發送到記錄再生部 300 之記錄再生部增號處理部 302，並使以該時間點 Ktes 用以接收被再增號化後之區段資訊點 Kbit 及存儲信息點 Kcon 的記錄再生部 300 之記錄再生部增號處理部 302，係在記錄再生部增號處理部 302 之增號／譯碼化部 308，以對照時間點 Ktes 將被增號化之

本圖格式使用中國國家標準 (GB2444 規格 (219 ~ 259 公量)) - 151 -

五、發明說明 (159)

區段資訊點 Kbit 及存儲信息點 Kcon，在相互延時時以進行共有放著的對照時間點 Ktes 並譯碼化。

進而，步驟 S208 中，以譯碼化後之區段資訊點 Kbit，在步驟 S202 用以譯碼化進行讀出後之區段資訊，尚有，記錄再生部 300 之記錄再生部增號處理部 302，係將譯碼化後之區段資訊點 Kbit，存儲信息點 Kcon 及區段資訊 BIT，在步驟 S202 變成被合於讀出後之集管的區段資訊點 Kbit，存儲信息點 Kcon 及區段資訊 BIT 進行保存後，又，記錄再生部 300 之控制部 301，係將被譯碼化後之區段資訊 BIT 由記錄再生部 300 之記錄再生部增號處理部 302 讀出後。

進而，在步驟 S209 中，記錄再生部增號處理部 302 之控制部 306，係由區段資訊點 Kbit，存儲信息點 Kcon 及區段資訊 (BIT)，用以生成核對值 B (ICV b)，核對值 B，係如圖 24 所示，將被保存於記錄再生部增號處理部 302 之內部記憶體 307 的核對值 B 生成點 Kicvb 取為處理，將由區段資訊點 Kbit，存儲信息點 Kcon 及區段資訊 (BIT) 所構成排他性邏輯和以 DES 進行增號化並加以生成，其次，在步驟 S210 中，用以比較核對值 B 與集管 (Header) 內之 ICV b，進行一致後時進到步驟 S211。

核對值 B、ICV b，係為了用以驗證區段資訊點 Kbit，存儲信息點 Kcon，區段資訊之更改的核對值，使生成後之核對值 B，與被寄納於集管 (Header) 內之核對

本圖格式使用中國國家標準 (GB2444 規格 (219 ~ 259 公量)) - 152 -

A7
B7

五、發明說明 (160)

值：ICVB 進行一致後時，係被判斷被保持於記錄裝置 400 後之資料中之區段資訊編號 Kbir，存儲信息編號 Kcon，區段資訊編號。

步驟 S211 中，記錄再生部被處理部 302 之控制部 301，係由記錄裝置 400 之外部記憶部 402 檢出讀出後之資料的系管部由處理方針 (Usage Policy) 取出利用限制資訊，使再生部之存儲信息進行判定並可利用記錄再生部 300 (利用限制資訊為 1)，或也可利用別的同樣之記錄再生部 300 (利用限制資訊為 0)，判定之結果，利用限制資訊為 1 時，使再生部之存儲信息可利用該記錄再生部 300 被設定利用限制時，則進到步驟 S213，而利用限制資訊為 0，即也可利用別的同樣之記錄再生部 300 決定時，則進到步驟 S215。向有，步驟 S212 之處理係進行記錄再生部被處理部 302

其次，步驟 S212 中，記錄再生部 300 之控制部 301，係由記錄裝置 400 之外部記憶部 402 檢出讀出後之資料的系管部由處理方針 (Usage Policy) 取出利用限制資訊，使再生部之存儲信息進行判定並可利用記錄再生部 300 (利用限制資訊為 1)，或也可利用別的同樣之記錄再生部 300 (利用限制資訊為 0)，判定之結果，利用限制資訊為 1 時，使再生部之存儲信息可利用該記錄再生部 300 被設定利用限制時，則進到步驟 S213，而利用限制資訊為 0，即也可利用別的同樣之記錄再生部 300 決定時，則進到步驟 S215。向有，步驟 S212 之處理係進行記錄再生部被處理部 302

A7
B7

五、發明說明 (161)

也可。

步驟 S213，係記錄再生部 300 之控制部 301，係將記錄再生部固有之核對值 ICDVdev 在記錄再生部 300 之記錄再生部被處理部 302 被進行計算，記錄再生部固有之核對值 ICDVdev，係如圖 25 所示將被保存於記錄再生部被處理部 302 之內部記憶部 307 的記錄再生部名稱 Kdev 做為輪匙，並在步驟 S211 將進行並行取索的內部核對值以 DES 進行暗號化加以生成。

其次，步驟 S214 中，在步驟 S213 用以比較進行計算後之記錄再生部固有之核對值 ICDVdev，及在步驟 S202 進行讀出後之無管內之 ICDVdev，在進行一致後時，進到步驟 S217。

另外在步驟 S215，係記錄再生部被處理部 302 之控制部 306，係在記錄再生部被處理部 302 之暗號化部 308 被檢出被對 ICDV 進行計算，暗號化部 ICDV，係如圖 25 所示，將被保存於記錄再生部被處理部 302 之內部記憶部 307 的系統管名稱 Ksys 做為輪匙，將中間核對值以 DES 進行暗號化加以生成。其次，步驟 S216 中，用以比較核對值之暗號化部 ICDV，及無管 (Header) 內之 ICDV，在進行一致後時，則進到步驟 S217。

繼續核對 ICDV，及記錄再生部固有之核對值 ICDVdev，係為用以驗證 ICDV，ICVB 各存儲信息段之核對值全部之區段的核對值，因此，藉由上述之處

A7
B7

五、發明說明 (162)

理裝被生成後之核對值被等於系管 (Header) 內後之核對值：ICVI 或 ICDVdev 在進行一致後時，係被判斷被等於於記錄裝置 400 後之 ICDV，ICVB，各存儲信息區段之核對值全部為一致。

接著，步驟 S217 中，記錄再生部 300 之控制部 301，係由記錄裝置 400 用以讀出區段資料，進而在步驟 S218 中用以判定是否暗號化，被暗號化時，則在記錄再生部 300 之記錄再生部被處理部 302 中進行區段資料之暗號化。未暗號化時，則進到步驟 S219 並進到步驟 S220。

其次，步驟 S220 中，記錄再生部 300 之控制部 301，係依據區段資訊 (BIT) 內之存儲信息區段資訊，判定存儲信息區段是否成爲暗號化對象，使存儲信息區段成爲暗號化對象時，在無管中之區段資訊中使存儲信息核對值被暗號化，使存儲信息區段成爲暗號化對象時，則在步驟 S221 中，使該區段之存儲信息區段之存儲信息核對值 ICDV，進行計算，使存儲信息區段未成爲暗號化對象時，則進到步驟 S221 及步驟 S222 並進到步驟 S223。

存儲信息核對值 ICDV，係如前面圖 36 之說明被段被暗號化時，以存儲信息編號 Kcon，將該被段之存儲信息區段以 DES 之 CBC 模式進行暗號化，將其結果全部以 8 組元單位進行暗號化並進行並行生成後之存儲信息中間值以被等於於記錄再生部 300 之內部記憶部

A7
B7

五、發明說明 (163)

307 後之存儲信息核對值生成輪匙 Kicv 進行暗號化並加以生成。又，該被段被暗號化時，則將資料 (平素文) 全部以 8 組元單位進行輸入於圖 36 所示區段被對值生成部 (DES-CBC-MAC，將存儲信息核對值生成輪匙 Kicv 做為輪匙) 被取取得暗號化。

步驟 S222 中，記錄再生部被處理部 302 之控制部 301，係用以比較生成後之存儲信息核對值 ICDV，及在步驟 S202 由記錄裝置 400 將被等於於進行讀取後之系管部之存儲信息核對值 ICDV，將其結果與於記錄再生部 300 之控制部 301，將此進行讀取後之記錄再生部 300 之控制部 301，係在驗證進行成功後時，在步驟 S223 中，在記錄再生部系統 RAM 上用以容納執行 (再生) 用存儲信息平素文資料，記錄再生部 300 之控制部 301，係進而用以取出下次之暗號對象存儲信息區段並在記錄再生部 300 之記錄再生部被處理部 302 被進行驗證，將全部之存儲信息區段進行驗證止至重複同樣之驗證為止，RAM 容納處理 (步驟 S224)。

向有，在步驟 S204，步驟 S210，步驟 S214，步驟 S216，步驟 S222 之中之一，未取核對值一致時則係為暗號化及再生處理。

步驟 S224 中判定區段讀出，則進到步驟 S225，使存儲信息 (假式，資料) 之執行，再生被開始。

A7
B7

五、發明說明(164)

以上，係格式形態0中之存儲信息資料的再生處理流程。

其次，對於格式形態1中之存儲信息資料的再生處理使用圖43加以說明，與上述之格式形態0之再生處理將不同點為中心加以說明。

步驟S201～步驟S217為止之處理，係與上述之格式形態0之再生處理同樣所以省略說明。

格式形態1，係步驟S231中，使用暗號化零件之區域被執行，並使零件ICV被生成，進而，步驟S232中，使區域ICV1被生成。如前面之說明，格式形態1中，係使區域內之零件中至少1個有被對該ICV1之對象資料時，則關於該區域存在儲信息被對該ICV1被定義，區域1中之零件1的相對值P-ICVij，係使零件1被暗號化時，將平常文（譯英文）全體以8單元位碼進行排他性邏輯和之後以存儲信息被對值生成該Kicv做為執行暗號化後之值被生成。又，使零件1未被暗號化時，則將資料（平常文）全體以8單元位輸入到該S36用米被暗號化後生成該DES-CBC-MAC，將存儲信息被對值生成該Kicv做為暗號化後之值被取得被生成。

進而，在1個之區域1內使單有被對對象（ICV標記=subject of ICV）的零件僅存在1個時，則以上述之方法將生成後之被對值P-ICVij運送再為區域之相對值ICV1。又，在1個之區域1內使單有被對對象（ICV標記=subject of ICV）的零件多數存在時，則將該

（本發明之技術方案之主要部分）

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

A7
B7

五、發明說明(165)

之零件被對值P-ICVij，將連結於零件號碼順序之資料做為對象資料（平常文）全體以8單元位輸入到該S36所示重複被對值生成部（DES-CBC-MAC，將存儲信息被對值生成該Kicv做為暗號化）後為取得被生成。此係，即前面圖37之說明。

在格式形態1，係以上述之程序被生成後之存儲信息被對值的比較處理在步驟S222形成被執行，以下之步驟S223以下的處理與格式形態0同樣所以省略說明。

其次，對於格式形態2中之存儲信息資料之再生處理使用圖44加以說明，與上述之格式形態0、1之再生處理將不同點為中心加以說明。

步驟S201～S210，係與上述之格式形態0、1之再生處理同樣所以省略說明。

格式形態2中，係在格式形態0、1中被執行之步驟S211～S216之處理未被執行。又，格式形態2中，係因尚未持有存儲信息被對值，所以在格式形態0、1中被執行後之步驟S222的存儲信息被對值之暗號化也未執行。

格式形態2之資料再生處理中，係步驟S210之被對值B的暗號化步驟後，進到步驟S217，經由記錄再生部300之控制部301的控制，使運送資料被運送。進而，步驟S241中，藉由記錄再生部300之記錄再生部暗號化處理部302使被包含於該對象資料之被對值Kbic的

（本發明之技術方案之主要部分）

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

打

A7
B7

五、發明說明(166)

該暗號化處理被執行，被容納於記錄長度400個之區域暗號Kbic，係以圖34所示存儲信息被對值Kcon被暗號化，在前述之步驟S207中使用該暗號化之存儲信息被對值Kcon進行區域暗號Kbic之譯碼。

其次，步驟S242中，在步驟S241使用被譯碼後之區域暗號Kbic使區域資料之譯碼處理被執行。進而，步驟S243中，使存儲信息（註文，資料）之執行，再生處理被執行。步驟S244中被判定全區被譯碼後以再生處理。

如此格式形態2之處理，係用以省略被對值等之被對值被暗號化處理，適合於高週率的譯碼處理之執行的構成，適合於被要求高速資料等實時處理之資料處理的構成。

其次對於格式形態3中之存儲信息資料之再生處理使用圖45加以說明，與上述之格式形態0、1、2之再生處理將不同點為中心加以說明。

格式形態3，係基本上與格式形態2中之處理與共同之部分較多，但格式形態3係如圖35中之說明未具有存儲信息被對值，又該區域暗號Kbic在記錄長度被以保存暗號Kicv被暗號化並被暗號化之點與格式形態2不同。

步驟S201～S210中，步驟S251、步驟S252、步驟S253、步驟S254之處理，係與前述之格式形態0、1、2中之處理處理不同為未合存儲信息被對值之處理被構成。

步驟S251中，記錄再生部300之控制部301

（本發明之技術方案之主要部分）

打

打

打

打

打

打

打

A7
B7

五、發明說明(167)

係由該暗號化之常數以記錄裝置固有之保存暗號Kicv用以取出被暗號化後之區域暗號Kbic，並運送到記錄再生部300之記錄與暗號控制部303進行發送到記錄再生部400。

由記錄再生部300用以接收被發來之區域暗號Kbic的記錄長度400，係將接收後之資料在記錄裝置暗號處理部401之暗號化部408，以保存於記錄裝置暗號處理部401之內部記憶長度400之記錄長度固有之保存暗號Kicv使進行譯碼化處理，在相互區區時以進行共有被對值之對話時暗號Kicv使進行可暗號化。該處理，係如前述之（8）互相互區區後之暗號化暗號處理已做詳細說明。

在步驟S252，記錄再生部300之控制部301，係通過記錄再生部300之記錄與暗號控制部303，由記錄長度400以對話時暗號Kicv用以接收被暗號化後之區域暗號Kbic。

其次，步驟S253中，記錄再生部300之控制部301，係以接收後之對話時暗號Kicv將被暗號化後之區域暗號Kbic運送到記錄再生部300之記錄再生部暗號處理部302，並以對話時暗號Kicv用以接收被暗號化後之區域暗號Kbic的記錄再生部300之記錄再生部暗號處理部302，係在記錄再生部暗號處理部302之暗號化部308，以對話時暗號Kicv將被暗號化後之區域暗號Kbic，在相互區區時以進行共有

（本發明之技術方案之主要部分）

打

打

打

打

打

打

打

A7
B7

五、發明說明 (172)

之生成處理態樣，係不限於上述方法有種種的生成處理態樣，並而有種種的驗證處理態樣，特別是存儲信息提供者或管理業者，及存儲信息利用者之關係中，可有以下說明之各種 I CV 生成及驗證處理態樣。

圖 46 ~ 圖 48 係顯示對於 I CV 之生成者中之生成處理，及藉由驗證者用以說明驗證處理態樣。

圖 46 係在上述之實施例中藉由說明之 DES-CBC 將 I CV 之生成處理，譬如以存儲信息提供者或管理業者進行 I CV 生成者，將生成後之 I CV 與存儲信息一起提供到記錄再生器利用者，即提供給驗證者之構成，該情形形成記錄再生器利用者，即驗證者在驗證處理時成為必要驗證，保管如被存於圖 18 所示內部記憶體 307 後之各被對準生成驗證，存儲信息利用者之驗證者（記錄再生器利用者），係使用被存於內部記憶體 307 後之該對準生成驗證，在驗證對準之資料適用 DES-CBC 並用以生成被對準與資料被對準用以執行比較處理，該情形，各被對準生成驗證，係被提供或 I CV 之生成者，驗證者做為檢查與有之驗證。

圖 47 係提供存儲信息提供者或管理業者之 I CV 的生成者藉由公開驗證時系統之數位等名用以生成 I CV，將生成後之 I CV 與存儲信息一起提供到存儲信息利用者，即驗證者、存儲信息利用者，即驗證者，係用以保存 I CV 生成者之公開驗證，並使用該公開驗證用以執行 I CV 之驗證處理的構成，該情形，存儲信息利用者（記

本國際式通用申請案名稱 (CN5NIA 規格 2210-237 公案) - 176 -

A7
B7

五、發明說明 (173)

錄再生器利用者），即驗證者具有之 I CV 生成者之公開驗證係不必儲存，管理係成為容易，使 I CV 之生成，管理在 1 個實體中被執行時等，使 I CV 之生成，管理適合以高安全地管理本進行時之態樣。

圖 48 係提供存儲信息提供者或管理業者之 I CV 的生成者藉由公開驗證時系統之數位等名用以生成 I CV，將生成後之 I CV 與存儲信息一起提供到存儲信息利用者，即驗證者，進而，使驗證者使用驗證者公開驗證者對於公開驗證證明書（譬如參考圖 14）與存儲信息資料一起提供到記錄再生器利用者，即驗證者，使 I CV 之生成者被存在時，各生成者，係將用以證明公開驗證之正確性的資料（公開驗證證明書）在驗證者管理中心進行作成。

I CV 之驗證者的存儲信息利用者，係持有驗證者管理中心之公開驗證，驗證者將公開驗證證明書之驗證藉由驗證者管理中心執行，使正確性被確認的話，用以取出被存於該公開驗證證明書後之 I CV 之生成者之公開驗證，進而，使用取出的 I CV 的生成者之公開驗證用以執行 I CV 之驗證。

該方法，係使 I CV 之生成者為多數，藉由用以執行此等之管理之中心被管理之執行系統在進行確立時有有效之態樣。

(12) 根據主驗證之明驗處理態樣生成構成

其次，本發明之資料處理系統中之特徵性的構成之一

本國際式通用申請案名稱 (CN5NIA 規格 2210-237 公案) - 176 -

A7
B7

五、發明說明 (174)

，對於根據主驗證之各種暗號處理態樣的生成構成加以說明。

使用如前圖面 18 之說明，在本發明之資料處理裝置中之記錄再生器 300 之內部記憶體，係使驗證的主驗證被對準，使用此等之各主驗證，譬如形成用以生成（參考圖 3）記錄驗證 Kke，並用以生成（參考圖 4）記錄驗證 Kdis 之構成。

先前，1 對 1 之實體態，即存儲信息提供者及存儲信息利用者，或，在上述之本發明之資料處理裝置中之記錄再生器 300 及記錄驗證 400 之間進行秘密通訊，相互驗證，以 A 生成，驗證時，係在各自實體間保持共同的秘密資訊，譬如使保持有驗證資訊，又，1 對多之關係，譬如 1 個之記錄再生器對多數之存儲信息利用者，或 1 個之記錄再生器對多數之記錄驗證等之關係中，全部之實體，即多數之存儲信息利用者，或多數之記錄驗證中使共有的秘密資訊，譬如使秘密資訊皆保持秘密構成，或，使 1 個之存儲信息提供者以個別用以管理多數之存儲信息利用者各自之秘密資訊（ex. 驗證），並將其關係在驗證信息利用者分別使用。

可是，如上述有 1 對多之利用關係時，則使全部用以所有共有的秘密資訊（ex. 驗證）的構成中，假使生 1 處之秘密資訊則利用相同秘密資訊者會全部受到影響之缺點，又，1 個之管理業者，譬如使存儲信息提供者以個別用以管理多數之存儲信息利用者各自之秘密資訊（ex. 驗證

本國際式通用申請案名稱 (CN5NIA 規格 2210-237 公案) - 177 -

A7
B7

五、發明說明 (175)

此），將使根據各存儲信息利用者分別使用做為構成，則用以識別全部之利用業者，且在其識別資料形成有必要對上對應固有秘密資訊（ex. 驗證）的名單，應與利用業者之增加會增加名單之管理管理負擔的缺點，在如此之實體間將秘密資訊共有之先前的問題點由主驗證之所有，及由主驗證藉由用以生成各驗證之驗證態樣的構成進行解決，以下對於該構成加以說明。

本發明之資料處理裝置中，係用以將驗證資訊或存儲信息之驗證，或在記錄再生器間使各種之暗號處理，驗證處理等中之不同個別的驗證形成必要時，將其個別之驗證，使驗證或驗證以固有秘密資訊資料（ID）等在個別資訊及記錄再生器 300 內使用最先決定之個別驗證生成方式進行生成，藉由該構成，一使生成後之個別驗證被對準時也能防止主驗證之洩漏，則形成可防止對系統整體的損害，又藉由主驗證經證明用以生成驗證之構成也成為不影響對多數者之管理。

對於具體之構成例，使用圖加以說明，首先，圖 49 係顯示將各種驗證使用記錄再生器 300 具有之各種主驗證用以說明生成之構成例，由圖 49 之底部 500，通訊裝置 600，係例及明之實體間而使用，使存儲信息輸入，存儲信息係藉由存儲信息驗證 Kcon 被暗號化，又，存儲信息驗證 Kcon，係藉由配送驗證 Kdis 被暗號化。

譬如，使記錄再生器 300 由驗證 500，通訊裝置

本國際式通用申請案名稱 (CN5NIA 規格 2210-237 公案) - 178 -

A7
B7

五、發明說明(180)

的處理例加以說明。

存儲信息製作或管理程序中之步驟 S511，係對存儲信息賦予識別子（存儲信息 ID）之步驟。步驟 S512，係由存儲信息製作或管理程序具有之複數的主軸（譬如複數之配速輪胎生成用主軸 MKdis）用以選擇 1 個之主軸的步驟。該選擇處理係使用 S52 通知加以說明，但對於對應於存儲信息之利用者的各圖、各權限、或機器類型等係先用以設定適用之主軸配速，依該設定進行執行主軸。

其次，在步驟 S513，係選擇在步驟 S512 選擇之主軸，及在步驟 S511 決定後之存儲信息 ID 用以生成暗號化用之輪胎。此係譬如，若做為用以生成配速輪胎 Kdis 之工程，則藉由 Kdis = DES (MKdisi, 存儲信息 ID) 加以生成。其次，步驟 S514 係將存儲信息之一部分，或全部藉由輪胎（譬如配速輪胎 Kdis）進行暗號化之步驟。存儲信息製作，係在步驟 S515 中，將存儲信息 ID，使用使之主軸及識別資訊，及暗號化存儲信息 ID 之配速輪胎 Kdis 進行暗號化處理後之存儲信息透過 DVD 等之媒體，通訊與遠端進行配速。

另外，譬如在配速再生後 300 等之利用有限權限，係步驟 S516 中，透過 DVD 等之媒體，通訊與遠端等對於該配速後之存儲信息資料中之主軸及識別資訊之主軸對於該是否自己所有加以判定，未持有對於該存儲信息資料中之主軸及識別資訊的主軸配速，則其配速存儲信息

本國式或適用中國專利第 CN1584 號 (2001.227 公告) - 183 -

A7
B7

五、發明說明(181)

，係在其利用權限中不能利用，並終了處理。

將對應於被配速後之存儲信息資料中之主軸及識別資訊之主軸係自己所有時，則在步驟 S517 中，透過媒體、通訊裝置等由被配速後之存儲信息資料中用以讀出存儲信息 ID，其次，在步驟 S518 中，根據讀出後之存儲信息 ID 及所有之主軸用以生成適用於暗號化存儲信息之暗碼，該生成處理，係取得配速輪胎 Kdis 之處理時，則譬如形成配速輪胎 Kdis = DES (MKdisi, 存儲信息 ID)。在步驟 S519，係使用該輪胎用以讀出存儲信息，並在步驟 S520 利用讀得存儲信息，即用以執行再生或播放。

在該例中，係如圖 1 下段所示，存儲信息製作或管理程序，係具有複數之主軸，譬如由複數之配速輪胎生成用主軸 MKdis 1 ~ n 所構成之主軸組態。另外，在利用該裝置 1 個之主軸配速具有 1 個之配速輪胎生成用主軸 MKdisi，使存儲信息製作或管理程序使用 MKdisi 係進行暗號化處理時，利用該裝置，係可利用以選擇其存儲信息。

做為該圖 51 所示之該處理態樣之具體例，係將適用各國不同主軸之例說明於圖 52。存儲信息提供者，係具有主軸 MK 1 ~ n，MK 1 係設定有配速於該日本之利用有限權限使用於用以執行存儲信息之暗號化處理的輪胎。譬如，由存儲信息 ID 及 MK 1 用以生成暗號化輪胎 K 1 並藉由 K 1 用以暗號化存儲信息，又，MK 2 係配速

本國式或適用中國專利第 CN1584 號 (2001.227 公告) - 184 -

A7
B7

五、發明說明(182)

於適合 US 之利用有限權限使用於用以執行存儲信息之暗號化處理的輪胎，而 MK 3 係配速於適合 US (歐洲) 之利用有限權限使用於用以執行存儲信息之暗號化處理的輪胎。

另外，適合日本利用有限權限，具體而言係在日本販賣之 P-C 或磁盤機等之配速再生時，係使主軸 MK 1 被容納於其內部記憶體，在適合 US 利用有限權限，係使主軸 MK 2 被容納於其內部記憶體，在適合 US 利用有限權限，係使主軸 MK 3 被容納於其內部記憶體。

在如此之構成中，存儲信息提供者，係將存儲信息與該可利用之利用有限權限，由主軸 MK 1 ~ n，以選擇性使用主軸用以執行配速於利用有限權限之存儲信息的暗號化處理。譬如將存儲信息 ID 係透過適用於適合日本之利用有限權限，係使用主軸 MK 1 用以生成暗號化處理的輪胎 Kdis，其次，步驟 S523，係將該暗號化處理之一部分，或全部藉由輪胎（譬如配速輪胎 Kdis）進行暗號化之步驟。暗號化處理，係經由如此之步驟用以供給於進行暗號化處理後之存儲信息資料之媒體。

另外，譬如在配速再生後 300 等之利用有限權限，係在步驟 S524 中，由被供給後之該輪胎用以讀出輪胎 ID。其次，在步驟 S525 中，根據讀出後之輪胎 ID 及所有之主軸用以生成適用於暗號化存儲信息之暗碼的輪胎。該生成處理，係取得配速輪胎 Kdis 之處理時，則譬如形成配速輪胎 Kdis = DES (MKdis, 輪胎 ID)。在步驟 S526，係使用該輪胎用以讀得存儲信息，並在步驟 S527 利用讀得存儲信息，即用以執行再生或播放。

其次，圖 53 係說明該裝置之圖，即將該裝置

本國式或適用中國專利第 CN1584 號 (2001.227 公告) - 185 -

A7
B7

五、發明說明(183)

ID 及主軸組合之處理例。於此，所謂該媒體係譬如用以容納 DVD、CD 等之存儲信息後之媒體。媒體 ID，係在 1 個 1 個之各媒體裝置固有也可，譬如，在該媒體之各製造此就係固有也可，如此做為媒體 ID 之分配方法可使用該方法。

存儲信息製作或管理程序中之步驟 S521，係對媒體用以決定識別子（媒體 ID）之步驟。步驟 S522，係根據存儲信息製作或管理程序具有之主軸及該 ID 用以生成暗碼用之暗碼於存儲信息等進行暗號化之輪胎的步驟。此係譬如，若做為用以生成配速輪胎 Kdis 之工程，則藉由該 Kdis = (MKdis, 媒體 ID) 用以生成配速輪胎 Kdis，其次，步驟 S523，係將該暗碼用之存儲信息之一部分，或全部藉由輪胎（譬如配速輪胎 Kdis）進行暗號化之步驟。暗號化處理，係經由如此之步驟用以供給於進行暗號化處理後之存儲信息資料之媒體。

另外，譬如在配速再生後 300 等之利用有限權限，係在步驟 S524 中，由被供給後之該輪胎用以讀出輪胎 ID。其次，在步驟 S525 中，根據讀出後之輪胎 ID 及所有之主軸用以生成適用於暗號化存儲信息之暗碼的輪胎。該生成處理，係取得配速輪胎 Kdis 之處理時，則譬如形成配速輪胎 Kdis = DES (MKdis, 輪胎 ID)。在步驟 S526，係使用該輪胎用以讀得存儲信息，並在步驟 S527 利用讀得存儲信息，即用以執行再生或播放。

本國式或適用中國專利第 CN1584 號 (2001.227 公告) - 186 -

A7
B7

五、發明說明(104)

在該例中，如圖 53 下段所示，媒體製作或管理者，及使用者裝置之雙方具有主輪匙，譬如配述輪匙生成用主輪匙 MKdis，在存儲信息之輪匙化，將該必要的配述輪匙分別送進進行所有之主輪匙保護各 ID（媒體 ID）加以生成。

該系統，係為一使媒體輪匙流給第三者時，使該系統內存儲信息之譯碼可能形成在第三者，但為了可用以防止該系統於保護 ID 之不同其他媒體之存儲信息的譯碼，可具有使 1 層之媒體輪匙之流給將影響到系統全體保護最小限度的效果。又，利用者裝置側，即記錄再生器中，也具有不需用以保持各媒體輪匙之對照名單的效果。又，以 1 層之媒體輪匙被輪匙化之存儲信息大小，係在其媒體內為了該限制於可容納之容量，為了避免攻擊達到必要的資訊可能性很少，所以可使得該譯碼之可能性減低。

其次，圖 54 係顯示記錄再生器側之處理順序，即記錄再生器 ID 及主輪匙結合之處處理。

記錄再生器利用者中之步驟 531，係譬如根據該容納於記錄再生器之內部記憶體的主輪匙及記錄再生器 ID 用以生成該存儲信息等進行輪匙化之輪匙的步驟，此係譬如，該容納用以生成存儲信息輪匙 Kcon 之工程，則藉由 $Kcon = DES (MKcon, 記錄再生器 ID)$ 用以生成該存儲信息輪匙 Kcon。其次，步驟 533，係將該容納存儲信息之一部分，或全部藉由輪匙（譬如配述輪匙 Kdis）進行

A. 該例式透過將主輪匙與媒體 ID (230 + RF 公鑰) - 107 -

A7
B7

五、發明說明(105)

輪匙化之步驟，步驟 533，係譬如將該存儲信息容納於硬碟等之記錄裝置。

另外，用以管理記錄再生器之系統管理側，係由用以容納存儲信息後之記錄再生器利用者裝置係將該容納資料之側，則步驟 534 中，由記錄再生器，讀出記錄再生器 ID。其次，步驟 535 中，將該讀出後之記錄再生器 ID 及所有之主輪匙用以生成該用於輪匙化存儲信息之復原的輪匙，該生成或處理，係取得存儲信息輪匙 Kcon 時，則譬如形成該存儲信息輪匙 $Kcon = DES (MKcon, 記錄再生器 ID)$ 。在步驟 536，使用該 Kcon 用以將該存儲信息。

在該例中，如圖 54 下段所示，記錄再生器利用者，及系統管理側之雙方具有主輪匙（譬如存儲信息輪匙生成用主輪匙 MKcon），在存儲信息之輪匙化，將該必要的配述輪匙分別送進進行所有之主輪匙保護各 ID（記錄再生器 ID）加以生成。

該系統，係為一使存儲信息輪匙流給第三者時，係該存儲信息之譯碼可能形成在第三者，但為了可用以防止該輪匙化於記錄再生器 ID 之不同其他記錄再生器後之存儲信息的譯碼，可具有使 1 個之存儲信息輪匙的復原影響到系統全體保護最小限度的效果。又，系統管理側，利用者裝置側兩者中，也具有不需用以保持各存儲信息輪匙之對照名單的效果。

圖 55 係具有，副裝置，譬如配述卡等之記憶裝置，

A. 該例式透過將主輪匙與媒體 ID (230 + RF 公鑰) - 108 -

A7
B7

五、發明說明(106)

及主輪匙，譬如應運使用記錄再生器間之相互認證處理將該輪匙生成主輪匙之構成。上述說明之認證處理（參照圖 20），係在對裝置之內部記憶體預先用以容納該輪匙後供使用，但於此圖 55 所示在該認證處理時該主輪匙可被生成之構成。

譬如記錄裝置之側裝置，係將該認證處理開始前之初級化處理，在步驟 541 中，將該容納於記錄裝置之副裝置的內部記憶體後之主輪匙及副裝置 ID 用以生成該認證輪匙 Kake 使用於相互認證處理，此係譬如，藉由 $Kake = DES (MKake, 副裝置 ID)$ 進行生成。其次，步驟 542 中，將生成後之該認證輪匙容納於記憶體。

另外，譬如在記錄再生器側之主裝置側，係步驟 543 中，該裝置後之記錄裝置，即由該裝置，通過該供裝置讀出副裝置 ID。其次，步驟 544 中，根據讀出後之副裝置 ID 及所有之該認證輪匙生成用主輪匙用以生成該認證輪匙適用於相互認證處理，該生成處理，係譬如形成該認證輪匙 $Kake = DES (MKake, 副裝置 ID)$ 。在步驟 545，使用該認證輪匙用以執行認證處理。

在該例中，如圖 55 下段所示，副裝置，及主裝置之雙方具有主輪匙，即該認證輪匙生成用主輪匙 MKake，在相互認證處理必要的該認證輪匙分別送進進行所有之主輪匙保護各 ID 加以生成。

該系統，係為一使該認證輪匙流給第三者時，該認證輪匙，係因該係在該例裝置，所以係在與該例裝置中

A. 該例式透過將主輪匙與媒體 ID (230 + RF 公鑰) - 109 -

A7
B7

五、發明說明(107)

，該認證形成不成立，由於該輪匙之流給具有該影響係為最小限度的效果。

因此，本發明之資料處理裝置中，存儲信息提供者及記錄再生器，或記錄再生器及記錄裝置之 2 個實體間中在有關該資料處理的手續時該必要之輪匙等的資訊由主輪匙及各 ID 值與該裝置進行生成之構成。因此，使該輪匙資訊由各實體即使用該，該經由該認證處理後該裝置側資訊固定，又如前述各該例裝置也形成不該認證名單之管理。

(13) 輪匙處理中之輪匙處理的控制

上述之實施例中，在記錄再生器 300 及記錄裝置 400 間之輪匙處理，係為了將該容易理解，主參是，使用該圖 7 藉由說明之第 DES 構成對於該輪匙處理之例做了說明。可是，本發明之資料處理裝置中被適用時該化處理方式係在上述之第 DES 方式不做任何限定，可用以採用該必要之安全狀態的輪匙化方式。

譬如該圖 8 已說明之圖 8-10 之構成適用三倍 DES 方式也可。譬如該圖 3 所示在記錄再生器 300 之輪匙處理部 302，及記錄裝置 400 之輪匙處理部 401 之雙方中，係可執行三倍 DES 方式之構成，在圖 8-10 藉由已說明之三倍 DES 方式可構成用以執行對應於該認證處理之處理。

可是，存儲信息提供者，係將該存儲信息用以優先處理後並將該存儲信息輪匙 Kcon 藉由第 DES 方式也有該為

A. 該例式透過將主輪匙與媒體 ID (230 + RF 公鑰) - 100 -

五、發明說明⁽¹⁸⁹⁾

6 4 位元輸出端構成之情形，又，用以使從安全性管理存儲信息輸出 Kcon 藉由三倍 DES 方式也有做為 128 位元輸出端構成之情形，或做為 192 位元，因此，將記錄再生部 300 之暗號處理部 302，及記錄裝置 400 之暗號處理部 401 之構成做為僅可對應於三倍 DES 方式，單 DES 方式其中一方之方式之構成係非發性，因此，記錄再生部 300 之暗號處理部 302，及記錄裝置 400 之暗號處理部 401，係做為皆可對應於單 DES，三倍 DES 之構成係為發性。

可是，將記錄再生部 300 之暗號處理部 302，及記錄裝置 400 之暗號處理部 401 的暗號處理構成為了能夠執行單 DES 方式，三倍 DES 方式之雙方之構成，係必須分別用以構成另外之電路，進而，譬如在記錄裝置 400 中為了用以執行對應於三倍 DES 之處理，係在於裝置 20 所示之指令地址必要形成於三倍 DES 之指令設定進行新的管轄，此係帶來形成構成於記錄裝置 400 之處處理的複雜化。

於此，本發明之資料處理裝置，係從單重暗號記錄裝置 400 側之暗號處理部 401 具有之選擇做為單 DES 構成，且可執行對應於三倍 DES 暗號化處理之處理，藉由三倍 DES 方式將暗號化資料（暗號，存儲信息）做為可容納於記錄裝置 400 之外部記憶部 402 的構成。

譬如圖 32 所示資料格式形態 0 之例中，由記錄再生部 300 對記錄裝置 400 用以執行存儲信息資料之下載。

本國際式通用申請書係根據 CINSAA 規格 (JIS X 2027 公案) - 191 -

五、發明說明⁽¹⁹⁰⁾

時，圖 39 係顯示前面已說明在格式形態 0 之下載流程的步驟 S101 用以執行認證處理，於此用以生成對話時間輸出 Kcon。進而，步驟 S117 中，在記錄再生部 300 側之暗號處理部 302 藉由對話時間輸出 Kcon 保存存儲信息輸出 Kcon 之暗號化處理而執行，而使從暗號化輸出端通過通訊線被轉送到記錄裝置 400，步驟 S118 中，使從接收暗號化輸出後之記錄裝置 400 之暗號處理部 403 藉由對話時間輸出 Kcon 用以執行存儲信息輸出 Kcon 之譯碼處理，進而，藉由保存輸出 Kstr 用以執行存儲信息輸出 Kcon 之暗號化處理，並將此發送到記錄再生部 300 之暗號處理部 302，之後，使記錄再生部 300 用以形成（步驟 S121）資料格式形態化後之資料發送到記錄裝置 400，而使記錄裝置 400 將接收後之資料進行管轄於外部記憶部 402。

上述處理中在步驟 S117、S118 間以地執行記錄裝置 400 之暗號處理部 401 的暗號處理構成以成為能夠執行單 DES，或三倍 DES 其中一方之方式，則使存儲信息提供與常用用以提供使用根據三倍 DES 之存儲信息輸出 Kcon 的存儲信息資料時，又用以提供使用根據 DES 之存儲信息輸出 Kcon 的存儲信息資料時，對各種情形形成可對應。

圖 56 係顯示本發明之資料處理裝置中使用記錄再生部 300 之暗號處理部 302，及記錄裝置 400 之暗號處理部 401 之雙方用以執行根據三倍 DES 方式的暗號

本國際式通用申請書係根據 CINSAA 規格 (JIS X 2027 公案) - 192 -

五、發明說明⁽¹⁹⁰⁾

處理方法用以說明構成之流程圖，圖 56，係做為一例由記錄再生部 300 將存儲信息資料在記錄裝置 400 進行下載時使用執行保存輸出 Kstr 及存儲信息輸出 Kcon 的暗號化處理部，顯示使存儲信息輸出 Kcon 藉由三倍 DES 方式之暗號化處理部，再者，於此，以存儲信息輸出 Kcon 為代價，顯示其處理部，但其他暗號，或存儲信息等，對於其他之資料也可同樣處理。

在三倍 DES 方式中，係如前面圖 8 ~ 10 中已說明，以單 DES 係 6 4 位元輸出端，藉由三倍 DES 方式時，係做為 128 位元，或 192 位元輸出端構成，使用 2 個，或 3 個之暗號處理，於此等之 3 個之暗號處理部分別做為 Kcon1、Kcon2、(Kcon3)，Kcon3 係有未使用時，所以用括弧顯示。

對於圖 56 之處理加以說明，步驟 S301 係在記錄再生部 300，及記錄裝置 400 間之相互認證處理步驟，該相互認證處理步驟，係藉由前面已說明圖 20 之處理而執行，尚有，該認證處理時，使對話時間輸出 Kcon 該生成。

終了步驟 S301 之認證處理，則在步驟 S302 中，使各該控制，該控制 A，該控制 B，存儲信息控制值，該控制值，各 ICV 之核對處理而執行。

終了此等之核對值 (ICV) 核對處理，則圖列定資料資料，則進到步驟 S303，在記錄再生部 300 中，記錄再生部暗號處理部 302 之控制部 306，係使用

本國際式通用申請書係根據 CINSAA 規格 (JIS X 2027 公案) - 193 -

五、發明說明⁽¹⁹¹⁾

記錄再生部暗號處理部 302 之暗號/譯碼化部 308，其使用前面輸出或生成後之認證輸出 Kdis，通過接收後之暗號 500，或，通訊部 305 由通訊裝置 500 進行被管轄於接收後之資料其實部的存儲信息輸出 Kcon 之譯碼化處理，該情形之存儲信息輸出，係藉由三倍 DES 方式之暗號，有存儲信息輸出 Kcon1、Kcon2、(Kcon3)，

其次，步驟 S304 中，記錄再生部暗號處理部 302 之控制部 306，係在記錄再生部暗號處理部 302 之暗號/譯碼化部 308 中，在步驟 S303 僅將譯碼化後之存儲信息輸出 Kcon1、Kcon2、(Kcon3) 之中的存儲信息輸出 Kcon1 在相互認證時以進行具有效率的對話時間輸出 Kcon 進行暗號化。

記錄再生部 300 之控制部 301，係以對話時間輸出 Kcon 兩合被暗號化後之存儲信息輸出 Kcon1 的資料由記錄再生部 300 之記錄再生部暗號處理部 302 譯出，將此等之資料通過記錄再生部 300 之記錄裝置控制部 303 發送到記錄裝置 400。

其次，步驟 S305 中，由記錄再生部 300 用以接收從裝置而來之存儲信息輸出 Kcon1 之記錄裝置 400，係將接收後之存儲信息輸出 Kcon1 在記錄裝置暗號處理部 401 之暗號/譯碼化部 406，相互認證時以具有效率的對話時間輸出 Kcon 進行譯碼化，進而，在步驟 S306 中，保存於記錄裝置暗號處理部 401 之內部記憶部 405 的記錄裝置固有之保存輸出 Kstr 使用暗號化。

本國際式通用申請書係根據 CINSAA 規格 (JIS X 2027 公案) - 194 -

A7
BT

五、發明說明(192)

透過通訊部404並發送到記錄再生部300。

其次，步驟S307中，記錄再生部將接收處理部302之控制部303，係在記錄再生部將接收處理部302之增號／譯碼化部306中，以步驟S303接收譯碼化後之存儲信息輸出Kcon1、Kcon2、(Kcon3)之中的存儲信息輸出Kcon2在相互認證時以進行共有放送的對話時間輸出Kses進行譯碼化。

記錄再生部300之控制部301，係以對話時間輸出Kses將含譯碼化後之存儲信息輸出Kcon2之資料由記錄再生部300之記錄再生部將接收處理部302讀出，並將此等之資料透過記錄再生部300之記錄裝置控制部303發送到記錄裝置400。

其次，步驟S308中，由記錄再生部300用以接收被發送而來之存儲信息輸出Kcon2後之記錄裝置400，係將接收後之存儲信息輸出Kcon2在記錄裝置將接收處理部401之增號／譯碼化部406，相互認證時以共有放送的對話時間輸出Kses進行譯碼化，進而，在步驟S309中，保存於記錄裝置將接收處理部401之內部記憶體405的記錄裝置固有之保存輸出Ksitr再將接收後，透過通訊部404並發送到記錄再生部300。

其次，步驟S310中，記錄再生部將接收處理部302之控制部303，係在記錄再生部將接收處理部302之增號／譯碼化部306中，以步驟S303接收譯碼化後之存儲信息輸出Kcon1、Kcon2、(Kcon3)

記錄再生部300之控制部301係以對話時間輸出Kses將含譯碼化後之存儲信息輸出Kcon2之資料由記錄再生部300之記錄再生部將接收處理部302讀出，並將此等之資料透過記錄再生部300之記錄裝置控制部303發送到記錄裝置400。

本國際式專利申請案係根據CNS/A4規格(210+207公案) - 192 -

A7
BT

五、發明說明(193)

之中的存儲信息輸出Kcon3在相互認證時以進行共有放送的對話時間輸出Kses進行譯碼化。

記錄再生部300之控制部301，係以對話時間輸出Kses將含譯碼化後之存儲信息輸出Kcon3之資料由記錄再生部300之記錄再生部將接收處理部302讀出，並將此等之資料透過記錄再生部300之記錄裝置控制部303發送到記錄裝置400。

其次，步驟S311中，由記錄再生部300用以接收被發送而來之存儲信息輸出Kcon3後之記錄裝置400，係將接收後之存儲信息輸出Kcon3在記錄裝置將接收處理部401之增號／譯碼化部406，相互認證時以共有放送的對話時間輸出Kses進行譯碼化，進而，在步驟S312中，保存於記錄裝置將接收處理部401之內部記憶體405的記錄裝置固有之保存輸出Ksitr再將接收後，透過通訊部404並發送到記錄再生部300。

其次步驟S313中，記錄再生部之增號處理部，係用以形成在圖32~35已說明之各種資料格式，並發送到記錄裝置400。

最後在步驟S314中，記錄裝置400，係將終了格式形成後之接收資料存儲於外部記憶體402，該格式資料，係在保存輸出Ksitr含有被譯碼化後之存儲信息輸出Kcon1、Kcon2、(Kcon3)。

藉由用以執行如此之處理，所容納於記錄裝置400之存儲信息輸出Kcon藉由三值DES方式之增號方式做為

記錄再生部300之控制部301係以對話時間輸出Kses將含譯碼化後之存儲信息輸出Kcon2之資料由記錄再生部300之記錄再生部將接收處理部302讀出，並將此等之資料透過記錄再生部300之記錄裝置控制部303發送到記錄裝置400。

訂

記錄再生部300之控制部301係以對話時間輸出Kses將含譯碼化後之存儲信息輸出Kcon2之資料由記錄再生部300之記錄再生部將接收處理部302讀出，並將此等之資料透過記錄再生部300之記錄裝置控制部303發送到記錄裝置400。

本國際式專利申請案係根據CNS/A4規格(210+207公案) - 193 -

A7
BT

五、發明說明(194)

輸出形成可進行容納，尚有，便容納信息輸出Kcon係Kcon1、Kcon2之2值輸出時，則步驟S310~312之處理被省略。

如此，記錄裝置400，係將容納後之處理，即步驟S305、S308之處理步驟藉由流水線式，係用以變更其對並流執行，其三值DES被適用之輸出形成可容納於記憶體，存儲信息輸出Kcon係DES之通用輸出時，則用以執行步驟S305、S306，並用以執行步驟S313之格式化處理而容納於記憶體即可，除此之外，係用以執行步驟S305、S308之處理的指令容納於前圖2已說明之圖29的指地處，將該處理藉由存儲信息輸出之態樣，即藉由三值DES方式，或單DES方式，進行通常1次~3次執行之構成即可，因此，在記錄裝置400之處理邏輯中不會三值DES之處理方式，形成可三值DES方式，單DES方式，雙方之處理，尚有，對於增號化方式，係記錄於存儲信息資料之管理部門的處理方針，並將此加以參考而進行判定。

(14) 記錄存儲信息資料之處理方針中之動態優先順位之程式控制處理

由於前已說明之圖4~圖6的存儲信息資料構成被理解，在被容納於本發明之資料處理裝置中利用存儲信息資料之管理部門之處理方針，係將存儲信息形態，動態優先順位資訊，本發明之資料處理裝置中之記錄再生部

記錄再生部300之控制部301係以對話時間輸出Kses將含譯碼化後之存儲信息輸出Kcon2之資料由記錄再生部300之記錄再生部將接收處理部302讀出，並將此等之資料透過記錄再生部300之記錄裝置控制部303發送到記錄裝置400。

本國際式專利申請案係根據CNS/A4規格(210+207公案) - 194 -

A7
BT

五、發明說明(195)

300，係使記錄於記錄裝置400，或DVD、CD，硬碟，進而磁卡匣等之各種記錄媒體後之可存取之存儲信息資料進行讀取時，將此等存儲信息之動態優先順位動態優先順位資訊加以決定。

記錄再生部300，係用各記錄裝置DVD與單、CD動態裝置，硬碟動態裝置等各種記錄裝置執行認證處理後，依據存儲信息資料中之優先順位資訊，用以優先並執行最高優先順位的存儲信息資料中之程序，以下對於該「根據在存儲信息資料之處理方針中之動態優先順位之程式控制處理」加以說明。

上述之不確定的資料處理與確實案例之說明中，係記錄再生部300由1個之記錄裝置400將存儲信息資料以進行所，執行時之處理中做了說明，可是，一般而論記錄再生部300，係如圖2所示除了記錄裝置400之外，透過讀取部304被連接DVD、CD、硬碟，並透過I/O111、S10112被連接記憶卡、磁卡卡匣等，在各種記錄媒體具有可存取之構成，還有，在圖2，係為了避免之重複化係記錄1個讀取部304，但記錄再生部300，係將不同記錄媒體，譬如DVD、CD、軟碟、磁碟以並列可供選。

記錄再生部300，係可存取於複數之記憶媒體，在分別之記憶媒體係分別存儲信息資料被容納，譬如便CD等外部之存儲信息提供係進行供給存儲信息資料，係以形成之圖4的資料構成被容納於記錄再生部300之媒體

記錄再生部300之控制部301係以對話時間輸出Kses將含譯碼化後之存儲信息輸出Kcon2之資料由記錄再生部300之記錄再生部將接收處理部302讀出，並將此等之資料透過記錄再生部300之記錄裝置控制部303發送到記錄裝置400。

訂

記錄再生部300之控制部301係以對話時間輸出Kses將含譯碼化後之存儲信息輸出Kcon2之資料由記錄再生部300之記錄再生部將接收處理部302讀出，並將此等之資料透過記錄再生部300之記錄裝置控制部303發送到記錄裝置400。

本國際式專利申請案係根據CNS/A4規格(210+207公案) - 195 -

五、發明說明 (196)

或通訊裝置進行下載時，則以圖 2 6、圖 2 7 之存儲信息資料構成被容納於記憶卡等之各記憶媒體，進而，具體而言，係根據存儲信息資料之格式形態如圖 3 2 ~ 3 5 所示在媒體上，以記錄裝置上分別以不同格式被容納。可是，不管在任何情形在存儲信息資料之集管中的處理方針係被含有存儲信息影響，而對該先開裝置中。

對此等，複數之存儲信息資料將可存取時之記錄再生器的存儲信息皆動處理依據流程圖加以說明。

圖 5-7 係圖示可停貯存儲信息有複數數之處處理例(1)之處處理流程圖。步驟 S611-1, 係依記錄再生藉 300 用以執行可存取之記錄裝置的磁阻處理之步驟。可存取之記錄裝置, 係含有記錄卡、DVD 裝置、CD 光碟、磁碟裝置、磁帶、譬如通過 PIO111、SIO112 被連接磁卡等。磁阻處理, 係在圖 5 所示控制部 301 之控制下對各記錄裝置如依排前面圖 20 已說明之程序被執行。

其次，參照 S 6 1 2 中，在進行認證成功後之記錄表
單內的記憶體由該容納後之存儲信息資料用以檢測可啓動
之程式。此係，具體而言，則係指會於存儲信息資料之處
理方針的存儲信息形態用以檢出具有程式做為處理被執行

其次，步驟 S 6 1 3 中，用以判定在步驟 S 8 2 1 被抽出後之可動之程式中之啓動優先順位。此係，具體而言，則用以比較被含於步驟 S 6 1 2 中被選擇後之複數可動

五、登明說明 (197)

助的存儲信息資料之舉管中的處理資訊之優先資訊並用以
選擇最高優先權位的處理。

接著在步驟 S 6 1 4 用以啓動被選擇後之程式，尚有，複數之可啓動的程式中被被設定後之優先順位有相同時，則在記錄裝置調用以設定省略之優先順位，用以執行被容納於被選擇優先順位後之存儲信息程式。

圖 5-8 係顯示在複數之記錄裝置用以設定識別子。在對於該附各識別子後之記錄裝置用以執行順序，認證處理。存儲信息程式檢索之處理態樣，即可信賴乎該信息有複數時之處理例（2）。

在步驟 S 6 2 1，係用以執行被裝著於記錄再生器 3 0 0 供之記錄裝置 (1) 的記錄處理 (參考圖 2 0) 之步驟，在複數 (n 個) 之記錄裝置係被賦予順序 1 ~ n 之識別子。

在步驟 S622，係用以判定在步驟 S621 是否經
 監成功，進行監成功時，則進到步驟 S623，由其監
 裝模 (I) 之記錄係集中則給與可變動處理。從現在
 進行成功時，則進到步驟 S627，用以判定有無的存
 儲信息可檢查之記錄係裝，無時則終了處理，而使記錄裝
 置存存時，則進到步驟 S628 用以更新記錄係裝置源引
 引。並是復步驟 S621 以後之監處理步驟。

步驟 S 6 2 3 中之處理，係由被容納於記錄裝置 (1) 後之存儲信息資料用以被測可啓動程式的處理。此係，具體而言，係使被含於存儲信息資料之處理方針的存儲價

五、發明說明 (108)

息形態用以抽出具有程式者做為處理被執行。

在步驟 S 6 2 4, 係保存儲信息形態用以判定是否被抽換具有複式者, 若抽換時, 則在步驟 S 6 2 5 中, 用以選擇抽換式中最為優先順位的程式, 並在步驟 S 6 2 6 中用以執行選擇程式。

步驟 S 6 2 4 中，使存儲信息形態被判定未被抽具有程式者之時，則進到步驟 S 6 2 7，用以判定有無新的存儲信息抽來之記錄裝置。無時則終了處理，而使記錄裝置存在時，則進到步驟 S 6 2 8 用以更新記錄裝置識別子，並重複步驟 S 6 2 1 以後之記錄處理步驟。

圖 59 係顯示可發動卡彈信息有底數時之處理例 (3) 之處理流程圖。步驟 S651，係使記錄再生 300 用可以執行存取之記錄裝置的認證處理之步驟。用以執行存取之 DVD 裝置、CD 光碟、硬盤裝置、記憶卡、遊戲卡匣等之認證處理。認證處理，係在圖 2 所示控制部 301 之控制下對各記錄裝置實如依據前面圖 20 已說明之程序進行之。

其次，步驟 S 6 5 2 中，由被告納於運行成功認證後之記憶裝置內的記憶體之存儲信息資料用以檢測可啟動的程式。此係，具體而言，使該含於存儲信息資料之處理方針的存儲信息形態用以輸出具有程式者做為處理並被執行。

其次，步驟 S 6 5 3 中，係在步驟 S 6 5 2 將被抽出之可啓動之程式的名稱等資訊顯示於顯示裝置。尚有，

五、發明說明 (199)

顯示裝置係在圖2並未顯示，但形成為使A/V輸出資料與振輸出後之資料接輸出於未圖示顯示裝置之構成。尚有，各存儲信息資料之程式名稱等之利用者資訊，係按收納於存儲信息資料之識別資訊中。在圖2所示主CPU10B之控制下通過控制部301將認證完成之各存儲信息資料之程式名稱等，程式資訊與輸出輸出裝置。

其次在步驟 S 6 5 4, 係由圖 2 所示輸入接口, 並制器、滑鼠、鍵盤等之輸入裝置藉由利用者將程式選擇輸入至選擇輸入接口 110 使主 CPU 106 進行接受, 依據選擇輸入, 在步驟 S 6 5 5 中用以執行利用者選擇程式。

如此本發明之資料處理裝置，係在接收信息資料中之某單元內的處理資訊時，以非動態方式將接收後資訊位置，並記錄該資訊產生 300 依據該資訊後測定位元以非動態方式，或在顯示裝置用以顯示啟動程式資訊藉由利用者被選擇之構成，所以使利用者不必力以檢索方式，形成可節省啟動所需之時間及利用者之勞力，又可動態式，使全部啟動於記錄裝置之認證處理後，或按形成有顯示可啟動程式，所以由用以選擇程式後進行正當性的確認等處理之煩雜性被消除。

(15) 存儲信息構成及再生(伸長)處理

本發明之資料處理裝置，係如上述之記錄再生器
300，由媒體500或通訊裝置600下載存儲信息，
再由記錄裝置400進行再生處理。上述之說明，係存儲

五、發明說明(200)

信息之下載，或隨等再生處理，將數位化資料之處理最爲中心做了說明。

圖3之記錄再生部300中之控制部301，係由用以提供所存儲信息資料之DVD等之裝置500、通訊裝置600、記錄裝置等存儲信息資料之下載處理，或再生處理以及控制部組成，將數位化、譯碼化處理全體。

做爲此等之處理結果被取得之可再生信息信息，係具有聲音資料、圖像資料等。譯碼資料係由控制部301該資料由圖2所示主CPU之控制下，根據聲音資料、圖像資料等被輸出到AV輸出部。可是，使存儲信息資料如聲音資料若使MP3被形成，則藉由圖2所示AV輸出部之MP3再將該聲音資料之譯碼處理形成被輸出。又，使存儲信息資料係圖像資料，若係MP2或MPEG圖像，則藉由AV處理部之MPEG2譯碼部使該譯碼處理形成被輸出。如此，被合於存儲信息資料之資料，則也有被壓縮(譯碼化)處理時，又也有未將該壓縮處理之資料，用以實施該存儲信息之處理加以輸出。

可是，壓縮處理、伸長處理等，係有種種的種類，由存儲信息提供被提供該壓縮資料也對該伸長處理進行時，會產生所不能進行之事態。

於此，本發明之資料處理裝置，係用請求在資料存儲信息中，一起用以收納該壓縮資料及其譯碼(伸長)處理程式之構成，或將該壓縮資料及譯碼(伸長)處理程式之處理資訊被存儲信息資料之無聲音資訊進行收納之構成。

五、發明說明(201)

由圖2所示之資料處理全體圖，所有構本構成之要素及圖樣要素以圖樣圖面顯示於圖60、記錄再生部300、係屬於DVD、CD等之裝置500、或通訊裝置600、或由用以收納存儲信息之記憶卡等之記錄裝置400接受種種之存儲信息之資料，此等之存儲信息，係有聲音資料、靜態圖像、動態圖像資料、程式資料等，又有實施壓縮處理、或未實施處理等，又，有被形成壓縮處理等，或未被形成等，包含種種的資料。

使接受存儲信息被輸出時，係藉由如上之項目中已說明之方法進行所部301之控制下，及該被處理部302之時被處理使譯碼處理被執行，被譯碼後之資料係在主CPU106之控制下被轉送到AV處理部109，並被收納於AV處理部109之記憶部3090後，在存儲信息解析部3091中使存儲信息被構成之解析被執行，譬如在存儲信息中若該資料伸長處理被收納，則在程式記憶部3093用以收納該資料，若該含有聲音資料、圖像資料等之資料則將此等被收納於資料記憶部3092，伸長處理部3094，係用以使用該被收納於該部記憶部後之MP3等伸長處理方式用以執行被收納於該部記憶部3092後之壓縮資料之伸長處理，並被輸出到聲音輸出部3001，並重3002。

其次，使AV處理部109通過控制部301對於接受之資料的構成及處理最優之例加以說明，得知，於此，由存儲信息之例係顯示聲音資料，又做爲壓縮處理之例

五、發明說明(202)

其適用MP3之壓縮程式爲代表加以說明，但本構成，係不僅聲音資料，也可適用於圖像資料，又，對於該伸長處理等不僅MP3，也可用以適用MPEG2、4等各樣式。

圖61係顯示存儲信息被構成例，圖61係藉由MP3再被壓縮後之聲音資料6102，MP3譯碼(伸長)處理方式6101合併成1個之存儲信息被構成之例，此等之存儲信息，係做爲1個存儲信息被收納於裝置500、或記錄裝置400、或由通訊裝置600被配到，記錄再生部300，係將此等之存儲信息如前圖已說明，若有被壓縮化者，則藉由伸長處理部303用以執行該譯碼處理後，被轉送到AV處理部109。

在AV處理部之存儲信息解析部3091，係用以解析該被收後之存儲信息，由聲音資料伸長程式(MP3譯碼部)部，及壓縮聲音資料部所構成存儲信息，用以取出聲音資料伸長程式(MP3譯碼部)部並在程式記憶部3093用以記憶該程式，將該聲音資料記憶於資料記憶部3092，所有，存儲信息解析部3091，係將存儲信息另外被收後之存儲信息名稱，用以接收存儲信息被構成資訊等之資訊，或根據顯示於該存儲信息內之資料名稱等類別資訊、資料長、資料構成等用以執行存儲信息解析也可，其次，壓縮伸長處理部3094，係將該被收納於該部記憶部3093後之聲音資料伸長程式(MP3譯碼部)用以執行該被收納於資料記憶部3092後之MP3類

五、發明說明(203)

聲音資料的伸長處理，而AV處理部109係伸長後之聲音資料輸出到聲音輸出部3001。

圖62係顯示有圖61顯示之存儲信息被構成資料之再生處理一例之流程圖，步驟S671，係將收納於AV處理部109之記憶部3090後之資料名稱，譬如含有聲音資料之存儲信息則將資料名稱之資訊與存儲信息另外被收後之資訊，或由存儲信息內之資料取出，並顯示於螢幕3002，步驟S672，係將利用者之選擇由該螢幕，被輸入到輸入裝置通過輸入接口進行接受，在CPU106之控制下根據利用者輸入資料再行處理指令輸出到AV處理部109，AV處理部109，係在步驟S673中藉由利用者選擇用以執行資料之輸出，伸長處理。

其次圖63係顯示在1個之存儲信息被包含壓縮聲音資料，或伸長處理方式之其中一方，並做爲將各存儲信息之無聲音資訊顯示存儲信息內之含有存儲信息被構成例。

如圖63所示，使存儲信息有程式6202時，則做爲無聲音資訊6201有程式，及程式名稱顯示有MP3伸長程式被含有存儲信息類別資訊。另外，將聲音資料6204做爲存儲信息含有時，則在螢幕6203之存儲信息資訊資訊具有MP3壓縮資料被含有資訊，該無聲音資訊，係如前述之圖4所示由該含有存儲信息資料所應之處理方針(參考圖5)中的資料用以選擇在再生必要的資訊轉送到AV處理部109並在存儲信息及進行增加可構成。

A7
BT

五、發明說明(204)

具體而言，係在圖5所示「處理方針」中之各構成資料在階段處理部302中成為必要之處理方針資料，及在AV處理部109中在再生處理時成為必要之資料以附加識別值，便此等識別值，在AV處理部109中根據顯示必要者進行輸出可成為無聲資訊。

圖63所示用以表示各存儲信息係之AV處理部109的存儲信息解析部3091，係依據無聲資訊，有程式則將程式存儲信息記憶於資料記憶部3092，之後，歷經伸長處理部3094，係由資料記憶部取出資料，並依據記憶於程式記憶部3093後之M/P3程式用以執行伸長處理並加以輸出，自有，左程式記憶部3093便已相同一般式被取時，則程式內容處理有略也可。

圖64係顯示具有圖63所示存儲信息構成資料之再生處理的一例流程圖，步驟S675，係被取於AV處理部109之記憶體3090後之資料名義，譬如若有存儲資料之存儲信息與前名等之資料則存儲信息另外取之資訊，經由存儲信息內之無聲取，並顯示於螢幕3002，步驟S676，係將利用者之選擇由開關，變換等各種輸入裝置通過輸入接口110進行接受。

其次，在步驟S677，係用以檢索則對於利用有選擇之資料再生用程式（譬如M/P3），該程式檢索對象，係將記錄於步驟300之可存取範圍作為最大檢索範圍為條件，譬如圖60所示也將各記憶500，通訊狀態

A7
BT

五、發明說明(205)

500，記錄裝置400等也做為檢索範圍。

被轉交到AV處理部109之存儲信息係係有資料部，程式存儲信息係也有被取於記錄再生部300內其他之記錄號碼時，透過DVD，CD等之區隔由存儲信息提供者也有被選定，因此，檢索對象係檢索範圍則用以記錄再生部300之存取容納範圍，使將檢索結果發現再生程序，則在CPU106之控制下根據利用者輸入資料將再生處理指令輸出到AV處理部109，AC處理部109，係由步驟S679中之利用者選擇用以執行資料之輸出，伸長處理，又，做為則的實施例，將程式之檢索在此步驟S675之前進行，步驟S675中，係使程式係成用以顯示被檢測之資料也可。

接著圖65係顯示在1層之存儲信息包含有無聲資訊資料6303，伸長處理程式6302，進而使資料存儲信息之無聲資訊6301包含有存儲信息之再生優先順位資訊的構成例，此係，在前圖61之存儲信息係成做為無聲資訊用以附加再生優先順位資訊之資訊，與前圖之「(14)存儲信息資料中根據處理方針中之資訊優先順位之程式資訊例」同樣，在接至AV處理部109後之存儲信息則根據被設定之再生優先順位用以決定再生順序。

圖66係顯示具有圖65所示存儲信息構成資料之再生處理的一例流程圖，步驟S681，係被取於AV處理部109之記憶體3090後之資料，即將再生對象資料

A7
BT

五、發明說明(206)

將之資料資訊設定於檢索名單，檢索名單係使用AV處理部109內之記憶體的一部分領域進行設定，其次，步驟S682中，由AV處理部109之存儲信息解析部3091中之檢索名單用以選擇高優先順位之資料，並在步驟S683中，用以執行選擇後之資料之再生處理。

其次圖67係顯示在1層之存儲信息係由無聲資訊及程式資料6402，或無聲資訊6403，及無聲資料6404之其中之一組合所構成例中，係在資料存儲信息之無聲6403，被附加有再生優先順位資訊之構成例。

圖68係顯示具有圖67所示存儲信息係成資料之再生處理的一例流程圖，步驟S691，係被取於AV處理部109之記憶體3090後之資料，即將再生對象資料之資料資訊設定於檢索名單，檢索名單係使用AV處理部109內之記憶體的一部分領域進行設定，其次，步驟S692中，由AV處理部109之存儲信息解析部3091中之檢索名單用以選擇高優先順位之資料。

其次，在步驟S693，係用以檢索則對於被選擇之資料的資料再生用程式（譬如M/P3），該程式檢索對象，係與前圖64之流程圖中之處理同樣，將記錄於再生部300之存取容納範圍做為最大檢索範圍為條件，譬如也將圖60所示各記憶500，通訊狀態600，記錄裝置400等做為檢索範圍。

做為檢索結果找到再生信息（在步驟S694 Yes），則在步驟S695中，將選擇後之資料使用

A7
BT

五、發明說明(207)

檢索結果被取得之程式，用以執行伸長再生處理。

另外，做為檢索結果檢索式未被檢測時（在步驟S694 Yes），則進到步驟S696，在步驟S691被檢於設定之檢索名單中之其他資料，使用同一程式之再生處理用以檢索必要的資料，此係，由明白顯示對新的資料即使用以再生程式檢索值也未檢出，進而，在步驟S697中用以判定檢索名單是否空，非空的情形，則返回到步驟S692，並用以輸出出其次的高優先順位之資料，用以執行程式檢索處理。

如此，若依據本構成，則被檢測處理後之存儲信息，與其詳細（伸長）程式一起被檢出，或係存儲信息係檢測後之資料，或係有伸長處理程式時，則分別在存儲信息具有無聲資訊則存儲信息有如何應處理資料，或用以執行如何之處理，所以接受存儲信息後之處理部（譬如AV處理部），係使用附屬於無聲資訊之伸長處理程式用以執行伸長再生處理，或將伸長處理程式與無聲資訊之無聲資訊進行檢索，並依據檢索結果被取得之程式用以執行伸長再生處理，所以藉由利用者成為不要資料之伸長程式的選擇，檢索等處理使用者負擔被減輕，可形成有效的資料再生，進而，在檢索若依據具有再生優先順位資訊之構成，則將再生順序形成可自動設定之構成，藉由利用者可省略再生順序設定之操作。

與有，上述之實施例，係係為檢索資料存儲信息，及型資料檢索資料之伸長處理程式則M/P3係為例做了

五、發明說明(208)

說明，但即要具有含壓縮資料存儲信息，應屬像資料之存儲處理之存儲信息同樣也可適用本構成，可造成同樣效果。

(18) 對存儲資料之生成及記錄裝置的容納、再生處理

本發明之資料處理裝置，係如使記錄再生部300中並執行之存儲信息有延遲程序等情形等，可將有將延遲方式在中途進行中斷，其定時間後，想應再開始時，則將其中斷時點之遊動狀態等存儲，即容納於記錄裝置，並將其再生時再進行輸出以進行游動之構成。

先前之遊動狀態，即人電腦等之記錄再生部中之存儲資料保存構成，係譬如內藏於記錄再生部，或持有在可外附之記錄卡、軟碟、磁碟卡等，或像磁帶等之記錄媒體用以保存存儲資料之構成，係特別此，對其存儲資料未具有安全確保構成，譬如在延遲應用程式以共同之規格形成進行資料之存儲處理的構成。

因此，譬如使用其1部之記錄再生部A發生被使用，或該被用之狀態，先期，存儲資料之安全性能性未被考慮係即於狀況。

本發明之資料處理裝置，係用以提供可實現如此之存儲資料之安全性能性之構成。譬如其遊動狀態之存儲資料，係係該狀態或係係可用之資料進行游動化並容納於記錄裝置，或，係係記錄再生部有之資料進行游動化並容納於記錄裝置，用此此等之方法，將存儲資料之利用

五、發明說明(209)

係可限制在特定之權限、特定之程式，使存儲資料之安全性能性確保，以下，對於本發明之資料處理裝置中之「對存儲資料之生成及記錄裝置之容納、再生處理」加以說明。

圖69係顯示對於本發明之資料處理裝置中之存儲資料容納處理加以說明之方塊圖。由DVD、CD等之媒體500，或通訊裝置600使存儲信息被提供到記錄再生部300，被提供存儲信息，係係由如前面說明之存儲信息具有游動之存儲信息編碼Kdev等游動化，記錄再生部300，在前進之「(7)」由記錄再生部對記錄裝置之下載處理」之關係保證說明(參考圖22)之處應用以取得存儲信息編碼，並將游動化存儲信息進行游動後，容納於記錄裝置400，於此，係係記錄再生部300將存儲信息程式由媒體、通訊裝置加以游動並進行再生，執行、執行後，將該取得存儲資料外掛，或容納於內藏之記錄卡、磁碟等之各游動記錄裝置400A、400B、400C其中之一，在再生處理，或將存儲信息在記錄裝置400A進行下載之後，由記錄裝置400A用以再生，執行存儲信息，並將其存儲資料外掛，或容納於內藏之記錄卡、磁碟等之各游動記錄裝置400A、400B、400C其中之一，在再生處理，或將存儲信息在記錄裝置400，對於再生之處理加以說明。

記錄再生部300，係如前面已說明具有用以生成記錄再生部識別IDdev，在系統內之等名輪胎的系統名輪胎Kxy，在圖內之記錄再生部有之等名輪胎的記錄再

五、發明說明(210)

在游動名輪胎Kdev，進而各名之游動名輪胎的主輪胎，對於主輪胎，係在「(12)」係游動主輪胎之游動處理編碼生成構成，中，如已詳細之說明，譬如，用以生成記錄裝置Kdis，或記錄裝置Kake等之輪胎。於此，並無特別以限定主輪胎之游動狀態用以代表記錄再生部300具有之主輪胎全盤以Kx加以顯示。在圖69之下載，係係存儲資料游動編碼Kxiv之游，存儲資料游動編碼Kxiv，係係存儲資料容納於各游動記錄裝置400A~C時之游動化處理，而且由各游動記錄裝置400A~C被應用於再生部之游動處理的游動編碼。使用圖70以下，用以說明存儲資料之容納處理及再生處理。

圖70係使用存儲信息具有游動，系統共同輪胎之其中之一游動存儲資料容納於記錄裝置400A~C其中之一的處理流程圖。尚有，各流程中之處理係執行記錄再生部300之處理，在各流程中以容納存儲資料之記錄裝置係內置，並有外掛記錄裝置400A~C其中之一部，可並無任何被限制。

步驟S701，係係存儲信息識別子，譬如再游動ID使記錄再生部300讀出之處理。此係，前面已說明之圖4、26、27、32~35所示被合於存儲信息資料中之游動資訊的資料，將存儲資料之容納處理指令游動圖2所示輸入接口110，由處理發生之主CPU106將存儲信息識別子之讀取控制於控制部301。

控制部301，係係執行程式透過DVD、CD-

五、發明說明(211)

ROM等，讀取部304被執行的存儲信息時，則透過讀取部304取出被合於存儲信息資料中之游動的游動資訊，並使執行程式，並容納於記錄裝置400後之存儲信息時，則透過記錄裝置控制部303取出被合於資訊，並有，係係記錄再生部300將存儲信息程式在執行中，已在記錄再生部中之RAM，其他可存儲記錄媒體使存儲信息識別子在被合於資訊時，則不執行游動的處理，而利用被合於讀取完成資料之游動資訊也可。

其次，步驟S702，係係由是否進行程式之使用限制用以變更處理之步驟。所謂程式使用限制，係係保存之存儲資料係在其式或游動係有可利利用以設定是否有限制的限制資訊，僅在程式式或游動係有可利利用時，係係為「有式使用限制」，並遊在程式式或游動係有可利利用時，係係為「無程式使用限制」。此係，係係利用係係為可任意設定也可，並使存儲信息製作進行設定，將游動資訊容納於存儲信息程式中或游動也可，被設定之後之限制資訊，係係在圖69之記錄裝置400A~C被為資料管理檔案被容納。

資料管理檔案之制顯示於圖71，資料管理檔案係係為項目並被為含資料號碼、存儲信息識別子，記錄再生部識別子，程式使用限制之游動信息生成、存儲信息識別子，係係被用以容納存儲資料之游動後之存儲信息程式的游動資訊。記錄再生部識別子，係係用以容納存儲資料後之記錄再生部之游動資訊，譬如在圖69所示(IDdev)，程式使

A7
BT

五、發明說明(212)

用限制，係如上述將保存之存儲資料僅在其程式做為固有可使用時，則做為「做」之設定，而未被限制於對應程式做為可利用時則形成「不做」之設定，程式使用限制，係用以利用存儲信息型別利用者可任意設定也可，並使存儲信息型別進行設定，將該資訊存納於存儲信息型別中亦可。

返回到圖 70，繼續流程之說明，在步驟 S702 中，對於程式使用限制被形成「做」之設定時，則到步驟 S703，係由存儲信息型別資料輸出存儲信息型別之資訊，譬如讀出前面已說明之存儲信息型別 Kcon 並將存儲信息型別資訊做為存儲資料時被輸出 Ksav，或將存儲信息型別資訊用以生成存儲資料時被輸出 Ksav。

另外，步驟 S702 中，對於程式使用限制被設定「不做」時，則到步驟 S707，在步驟 S707，係將資訊於記錄再產生 300 內之系統共同編號，譬如將系統等名義 Krys 由記錄再產生 300 之內部記憶體 307 進行讀出，將系統等名義 Krys 直接寫入存儲資料時被輸出 Ksav，或將系統等名義輸出用以生成存儲資料時被輸出 Ksav，或，另外，保存於記錄再產生 300 之內部記憶體 307 內放著，與其他之編號所別之編號輸出做為存儲資料時被輸出 Ksav 也可。

其次，步驟 S704 中，以步驟 S703，或步驟 S707 選擇，或使使用生成後之存儲資料時被輸出 Ksav 用以執行存儲資料之暗號化處理，即暗號化處理，係使要

本國式處理用中國國家標準 (GB2818-2007) 公告 - 215 -

A7
BT

五、發明說明(213)

2 中之暗號化處理部 302 告知用以適用並執行前述 DES 算法。

步驟 S704 中被暗號化處理後之存儲資料，係將資訊於步驟 S705 中之記錄裝置，將存儲資料係可串納之記錄裝置如圖 69 所示具有雙數時，則使用將記錄裝置 400A~C 之其中之一做為存儲資料資訊於串納預先進行選擇，進而，在步驟 S706 中使用前面圖 71 在已說明之資料管理檔案以前而步驟 S702 設定後之程式使用限制資訊之寫入，即用以執行程式使用限制「做」或「不做」的寫入。

以上，使存儲資料之資訊處理進行終了，步驟 S702 中之 Yes，即「進行程式使用限制」之選擇被形成，根據步驟 S703 中之存儲信息型別有輸出而由生成後之存儲資料時被輸出 Ksav 被暗號化之存儲資料，係藉由未持有存儲信息型別有輸出資訊之存儲信息型別形成不可運轉處理，存儲資料係具有相同存儲信息型別資訊形成可用存儲信息型別，但，於此，存儲資料時被輸出 Ksav 係根據記錄裝置固有之資訊來被生成，所以譬如被容納於記憶十等之可被讀的記錄裝置後之存儲資料係在不再記錄再產生中包同對置之存儲信息型別一起進行使用而資訊形成可再生。

又，步驟 S702 中之 No，即被形成「不做」之程式使用限制，則根據步驟 S707 中之系統共同編號則由存儲資料時被輸出 Ksav 被暗號化處理後之存儲資料

本國式處理用中國國家標準 (GB2818-2007) 公告 - 216 -

A7
BT

五、發明說明(214)

係保存存儲信息型別子使用不問程式時，又，使記錄再產生發生不問時再產生形成可利用。

圖 72 係示理由圖 70 之存儲資料資訊處理用以將生成被容納後之存儲資料處理的說明。

步驟 S711，係由存儲信息型別資料，譬如將記錄 ID 從記錄再產生 300 讀出處理，此係，將前面已說明之圖 70 中存儲信息型別資訊之步驟 S701 同段之處理，將被容納於存儲信息型別中之資訊資訊的資料讀出處理。

其次，在步驟 S712，係由圖 69 所示記錄裝置 400A~C，使用圖 71 讀出已說明之資料管理檔案，並在步驟 S711 中用以抽出輸出後之存儲信息型別子，及進行對應被設定後之程式使用限制資訊，使被設定於資料管理檔案後之程式使用限制有「做」時，則到步驟 S714，有「不做」時，則到步驟 S717。

步驟 S714，係由存儲信息型別資料以讀出存儲信息型別之資訊，譬如用以讀出前面已說明之存儲信息型別 Kcon 並將存儲信息型別資訊做為存儲資料時被輸出 Ksav，或將存儲信息型別資訊用以生成存儲資料時被輸出 Ksav，該暗號化輸出被生成處理，係對於暗號化輸出被生成處理適用處理方法，根據其存儲信息型別有輸出被暗號化後之資料，根據同一之存儲信息型別有輸出經由被生成後之暗碼輸出形成可暗碼處理用暗碼化輸出被生成處理。

另外，步驟 S712 中，使資料管理檔案之設定對於程式使用限制設定有「不做」時，則在步驟中 717 中，

本國式處理用中國國家標準 (GB2818-2007) 公告 - 217 -

A7
BT

五、發明說明(215)

資訊於記錄再產生 300 內之系統共同編號，譬如將系統等名義 Krys 由記錄再產生 300 之內部記憶體 307 讀出，並將系統等名義 Krys 做為存儲資料時被輸出 Ksav，或根據系統等名義 Krys 用以生成存儲資料時被輸出 Ksav，又，另外，保存於記錄再產生 300 之內部記憶體 307 內放著，與其他之編號所別之編號輸出做為存儲資料時被輸出 Ksav 使用也可。

其次，步驟 S715 中，以步驟 S714，或步驟 S717 選擇，或使使用生成後之存儲資料時被輸出 Ksav 用以執行存儲資料之暗碼化處理，在步驟 S716 中，將暗碼後之存儲資料在記錄再產生 300 中進行再生，執行。

在以上，使存儲資料之再生處理進行終了，如上述在資料管理檔案被形成有「進行程式使用限制」時，則根據存儲信息型別有輸出被生成存儲資料時被輸出 Ksav，設定有「不進行程式使用限制」時則根據系統共同編號使存儲資料時被輸出 Ksav 被生成，被設定有「進行程式使用限制」時，使用之存儲信息型別之存儲信息型別子不相同則形成不能取得可存儲資料之暗碼處理的暗碼化輸出，形成可將存儲資料之安全性。

第三，圖 74 係使用存儲信息型別子用以生成存儲資料之暗碼化輸出，暗碼化輸出之存儲資料資訊處理流程 (圖 73)，存儲資料再生產處理流程 (圖 74)。

圖 73 中，步驟 S721~S722，係與圖 70 之

本國式處理用中國國家標準 (GB2818-2007) 公告 - 218 -

五、發明說明 (216)

步驟 S 7 0 1 ~ S 7 0 2 同樣之處理，所以省略說明。

圖 7 3 之存儲資料容納處理流程，係步驟 S 7 2 2 中進行「進行程式使用限制」時，在步驟 S 7 2 3 中由存儲信息資料之存儲信息識別子，即用以讀出存儲信息 ID 並將存儲信息 ID 值為存儲資料暗號輸出 Ksav，並根據存儲信息 ID 用以生成存儲資料暗號輸出 Ksav。譬如記錄再生器 300 之暗號處理部 307 係由存儲信息資料在讀出存儲信息 ID 後，適用被容納於記錄再生器 300 之內部記憶體後的主輸出 M K X，譬如藉由 D E S (M K X，存儲信息 ID) 可取得存儲資料暗號輸出 Ksav。或，另外，保存於記錄再生器 300 之內部記憶體 307 內取等，與其他暗號所判的暗號輸出值為存儲資料暗號輸出 Ksav 使用也可。

另外，步驟 S 7 2 2 中，對於程式使用限制做為「不做」時，則步驟 S 7 2 2 中，被容納於記錄再生器 300 內之系統共輸出，譬如將系統名輸出 Ksys 由記錄再生器 300 之內部記憶體 307 讀出，並將系統名輸出 Ksys 做為存儲資料暗號輸出 Ksav，或根據系統名輸出用以生成存儲資料暗號輸出 Ksav。或，另外，保存於記錄再生器 300 之內部記憶體 307 內取等，與其他暗號所判的暗號輸出值為存儲資料暗號輸出 Ksav 使用也可。

步驟 S 7 2 4 以下之處理，係與前述之圖 7 0 的處理流程中之步驟 S 7 0 4 以下之處理同樣，所以省略說明。

進而，圖 7 4 係以圖 7 3 之存儲資料容納處理流程使用

圖 7 3 係以圖 7 0 之存儲資料容納處理流程使用

本願書式適用中國專利法第 2 條 (CNSDA 規格 1300+200 公厘) - 216 -

五、發明說明 (217)

以再生，執行被容納於記錄裝置後之存儲資料的處理流程。步驟 S 7 3 1 ~ S 7 3 3 係與前述圖 7 2 之對應處理同樣，僅係步驟 S 7 3 4 不同。步驟 S 7 3 4 中，係由存儲信息資料用以讀出存儲信息識別子，即用以讀出存儲信息 ID 並將存儲信息 ID 值為存儲資料暗號輸出 Ksav，或根據存儲信息 ID 用以生成存儲資料暗號輸出 Ksav。該暗號輸出值生成後，係透過對應於暗號輸出值生成處理之處理部，根據其存儲信息識別子暗號輸出值之資料，係根據同一之存儲信息識別子經由生成後之暗號輸出形成可透過新適用暗號輸出值生成算法。

以下之處理，步驟 S 7 3 5，S 7 3 6，S 7 3 7，係與圖 7 2 之對應處理同樣所以省略說明。依據圖 7 3，圖 7 4 之存儲資料及再生處理，則進行程式使用限制之設定時，用以使用存儲信息 ID 並做為用以生成存儲資料暗號輸出，暗號輸出值之生成，所以與使用前圖之存儲信息有給定的存儲資料時，再生處理同樣，對照之存儲信息生成進行整合情形以外，係形成不能利用存儲資料之構成，或為可保存從前存儲資料安全。

圖 7 5，圖 7 7 係使用記錄再生器固有暗號輸出以生成存儲資料之暗號輸出，暗號輸出值之存儲資料容納處理流程 (圖 7 5)，存儲資料再生處理流程 (圖 7 7)。

圖 7 5 中，步驟 S 7 4 1，係與圖 7 0 之步驟 S 7 0 1 同樣的處理，所以省略說明。步驟 S 7 4 2，係

圖 7 5 係以圖 7 0 之存儲資料容納處理流程使用

圖 7 7 係以圖 7 0 之存儲資料容納處理流程使用

本願書式適用中國專利法第 2 條 (CNSDA 規格 1300+200 公厘) - 220 -

五、發明說明 (216)

所以設定要進行記錄再生器之限制之步驟，記錄再生器限制，係用以限定可利用存儲資料之記錄再生器時，即，用以生成存儲資料係在容納後之記錄再生器時做為可利用時設定為「做」，而在其他之記錄再生器時做為不可利用時設定為「不做」。步驟 S 7 4 2 中進行設定「進行記錄再生器限制」，則與前述步驟 S 7 4 3，進行設定「不做」則與前述步驟 S 7 4 7。

資料管理標準之對象係於圖 7 6，資料管理標準係為項目含資料號碼，存儲信息識別子，記錄再生器識別子，記錄再生器限制後再讀表被生成，存儲信息識別子，係做為用以容納存儲資料之對象後的存儲信息識別子之識別子，記錄再生器識別子，係用以容納存儲資料後之記錄再生器的識別子，譬如圖 8 9 所示之「IDdev」。記錄再生器限制，係用以限定可利用存儲資料之記錄再生器時，即用以生成存儲資料係在容納後之記錄再生器時做為可利用時進行設定「做」，而在其他之記錄再生器時做為不可利用時進行設定「不做」。記錄再生器限制資訊，係利用存儲信息生成式使用者可任意設定也可，並在存儲信息生成者進行設定，將該資訊容納於存儲信息生成式中做等也可。

圖 7 5 之存儲資料容納處理流程中，係步驟 S 7 4 2 中，進行「進行記錄再生器限制」之設定時，在步驟 S 7 4 3 中由記錄再生器 300 用以讀出記錄再生器固有暗號，譬如將記錄再生器名輸出 Kdev 由記錄再生器 300 之內部記憶體 307 讀出並將記錄再生器名輸出 Kdev

圖 7 6 係以圖 7 0 之存儲資料容納處理流程使用

本願書式適用中國專利法第 2 條 (CNSDA 規格 1300+200 公厘) - 221 -

五、發明說明 (219)

Kdev 做為存儲資料暗號輸出 Ksav，或根據記錄再生器名輸出 Kdev 用以生成存儲資料暗號輸出 Ksav。或，另外，保存於記錄再生器 300 之內部記憶體 307 內取等，與其他暗號所判的暗號輸出值為存儲資料暗號輸出 Ksav 使用也可。

另外，步驟 S 7 4 2 中，對於記錄再生器限制做為設定「不做」時，係在步驟 S 7 4 7 中，被容納於記錄再生器 300 內之系統共輸出，譬如將系統名輸出 Ksys 由記錄再生器 300 之內部記憶體 307 讀出，並將系統名輸出 Ksys 做為存儲資料暗號輸出 Ksav，或根據系統名輸出用以生成存儲資料暗號輸出 Ksav。或，另外，保存於記錄再生器 300 之內部記憶體 307 內取等，與其他暗號所判的暗號輸出值為存儲資料暗號輸出 Ksav 使用也可。

步驟 S 7 4 4，S 7 4 5 之處理，係與前述之圖 7 0 的處理中之對應處理同樣，所以省略說明。

在步驟 S 7 4 6，係在資料管理標準 (參考圖 7 6) 將入存儲信息識別子，記錄再生器識別子，而且在步驟 S 7 4 7 使用將容納入設定後之記錄再生器限制資訊「做」/「不做」。

進而，圖 7 7 係在圖 7 5 之存儲資料容納處理流程中以再生，執行被容納於存儲資料的處理流程。步驟 S 7 5 1 係與前述之圖 7 2 之對應處理同樣，用以讀出存儲信息識別子，其次，步驟 S 7 5 2 中，係用以讀出存儲

圖 7 5 係以圖 7 0 之存儲資料容納處理流程使用

圖 7 7 係以圖 7 0 之存儲資料容納處理流程使用

本願書式適用中國專利法第 2 條 (CNSDA 規格 1300+200 公厘) - 222 -

A7
B7

五、發明說明(220)

納於記錄再生器 300 之內部記憶體後之記錄再生器識別子 (IDdev)。

在步驟 S 753，係由資料管理單元 (參照圖 7B) 用以讀出存儲信息識別子、記錄再生器識別子，並完成之記錄再生器限制資訊「做」或「不做」之各資訊，使資料管理單元中之存儲信息識別子進行一致性的項目中，使記錄再生器限制資訊被設定於「做」時，則使重要項目之記錄再生器識別子至步驟 S 752 與被讀取後之記錄再生器識別子不同則進行終了處理。

其次，在步驟 S 754 使資料管理單元之設定有「進行記錄再生器限制」時，則進到步驟 S 755，有「不做」時，則進到步驟 S 758。

步驟 S 755 中，係由記錄再生器 300 用以讀出記錄再生器識別子，譬如將記錄再生器名稱 Kdev 由記錄再生器 300 之內部記憶體 307 進行讀出並將記錄再生器名稱 Kdev 做為存儲資料譯碼化輪匙 Ksav，或根據記錄再生器名稱 Kdev 用以生成存儲資料譯碼化輪匙 Ksav，該譯碼化輪匙生成處理，係採用對於譯碼化輪匙生成處理的處理算法，根據其記錄再生器識別子被譯碼化後之資料，係根據同一之記錄再生器識別子藉由生成後之譯碼化輪匙形成可譯碼者並適用譯碼化輪匙生成算法，或，另外，係存於記錄再生器 300 之內部記憶體 307 內放著，與其他輪匙辨別的輪匙輪匙做為存儲資料譯碼化輪匙 Ksav 使用也可。

▲此模式適用於中國國家標準 (GB4836 規格 (230+237 公厘)) - 223 -

A7
B7

五、發明說明(221)

另外步驟 S 758 中，係按容納於記錄再生器 300 後之系統圖輪匙，譬如將系統名稱 Ksys 由記錄再生器 300 之內部記憶體 307 進行讀出，並將系統名稱 Ksys 做為存儲資料譯碼化輪匙 Ksav，或根據系統名稱 Ksys 用以生成存儲資料譯碼化輪匙 Ksav，或，另外，存於記錄再生器 300 之內部記憶體 307 內放著，與其他輪匙辨別的輪匙輪匙做為存儲資料譯碼化輪匙 Ksav 使用也可，以下之步驟 S 756、S 757，係與前述之存儲資料再生處理流程之對應步驟同様の處理。

圖 75，圖 76 所示之存儲資料，係依據再生處理流程，則被形成「進行記錄再生器限制」之選擇後存儲資料，係藉由記錄再生器內有輪匙，為了執行譯碼化處理，持有同一之記錄再生器識別子之記錄再生器，即係由同一之記錄再生器形成可利用進行譯碼。

其次，圖 78，圖 79 係指示使用記錄再生器識別子用以生成存儲資料譯碼化，譯碼化輪匙並進行容納，再生之處理。

圖 78 係使用記錄再生器識別子進行存儲資料之譯碼化並容納於記憶體，步驟 S 761~763，係從圖 75 選擇之處理，在步驟 S 764，係使用由記錄再生器讀出後之記錄再生器識別子 (IDdev) 用以生成存儲資料譯碼化輪匙 Ksav，將 IDdev 做為存儲資料譯碼化輪匙 Ksav 進行使用，或用以選擇容納於記錄再生器 300 之內部記憶體後之主輪匙 MKx，藉由 DES (MKx, IDdev) 取

▲此模式適用於中國國家標準 (GB4836 規格 (220+237 公厘)) - 224 -

A7
B7

五、發明說明(222)

將存儲資料譯碼化輪匙 Ksav 等，或，另外，係存於記錄再生器 300 之內部記憶體 307 內放著，與其他輪匙辨別的輪匙輪匙做為存儲資料譯碼化輪匙 Ksav 使用也可。

以下之處理步驟 S 765~S 768，係與前述圖 75 之對應處理同様の，所以省略說明。

圖 79 係藉由圖 78 之處理用以再生，執行後容納於記錄再生器後之存儲資料的處理流程圖，步驟 S 771~S 774，係與前述圖 77 之對應處理同様の。

在步驟 S 775，係使用由記錄再生器讀出後之記錄再生器識別子 (IDdev) 並用以生成存儲資料譯碼化輪匙 Ksav，將 IDdev 做為存儲資料譯碼化輪匙 Ksav 進行適用，或用以適用容納於記錄再生器 300 之內部記憶體後之主輪匙 MKx，藉由 DES (MKx, IDdev) 取得存儲資料譯碼化輪匙 Ksav 等，根據 IDdev 用以生成存儲資料譯碼化輪匙 Ksav，該譯碼化輪匙生成處理，係採用對於譯碼化輪匙生成處理的處理算法，根據其記錄再生器識別子被譯碼化後之資料，係根據同一之記錄再生器識別子藉由生成後之譯碼化輪匙形成可譯碼者並適用譯碼化輪匙生成算法，或，另外，係存於記錄再生器 300 之內部記憶體 307 內放著，與其他輪匙辨別的輪匙輪匙做為存儲資料譯碼化輪匙 Ksav 使用也可。

以下之處理步驟 S 776~S 778，係與前述圖 76 之對應處理同様の，所以省略說明。

圖 78、圖 79 所示之存儲資料容納，即依據再生處理

▲此模式適用於中國國家標準 (GB4836 規格 (230+237 公厘)) - 225 -

A7
B7

五、發明說明(223)

處理流程，則被形成「進行記錄再生器限制」之選擇後的存儲資料，係藉由記錄再生器內有輪匙，為了執行譯碼化處理，持有同一之記錄再生器識別子之記錄再生器，即係由同一之記錄再生器形成可利用進行譯碼。

其次使用圖 80~82，將上述之程式使用限制，及記錄再生器使用限制合併進行執行對於存儲資料，再生處理加以說明。

圖 80 係存儲資料容納處理，步驟 S 781 中，將存儲信息識別子由存儲信息資料讀出，步驟 S 782 中，進行程式使用限制判定，步驟 S 783 中進行記錄再生器限制判定。

「有程式使用限制」且「有記錄再生器限制」時，係在步驟 S 785 中，根據存儲信息識別子 (ex.Kcon)，及記錄再生器內有輪匙 (Kdev) 雙方生成存儲資料譯碼化輪匙 Ksav。此係，譬如 Ksav = (Kcon XOR Kdev)，或用以適用容納於記錄再生器 300 之內部記憶體後之主輪匙 MKx 並藉由 Ksav = DES (MKx, Kcon XOR Kdev) 可取解，或，另外，係存於記錄再生器 300 之內部記憶體 307 內放著，與其他輪匙辨別的輪匙輪匙做為存儲資料譯碼化輪匙 Ksav 使用也可。

「有程式使用限制」且「無記錄再生器限制」時，係在步驟 S 786 中，將存儲信息識別子 (ex.Kcon) 做為存儲資料譯碼化輪匙 Ksav，或根據存儲資料內有輪匙 (ex.Kcon) 用以生成存儲資料譯碼化輪匙 Ksav。

▲此模式適用於中國國家標準 (GB4836 規格 (230+237 公厘)) - 226 -

A7
B7

五、發明說明(224)

「無程式使用限制」且「有記錄再生限制」時，係在步驟 S 7 8 7 中，將記錄再生器間有輸出 (Kdev) 做為存儲資料增設輸出 Ksav，或根據記錄再生器間有輸出 (Kdev) 用以生成存儲資料增設輸出 Ksav，或，另外，保存於記錄再生器 300 之內部記憶體 307 內數據，與其他輸出到增設輸出做為存儲資料增設輸出 Ksav 使用也可。

「無程式使用限制」且「無記錄再生限制」時，係在步驟 S 7 8 7 中，系統共同輸出，譬如將系統名稱輸出 Ksys 做為存儲資料增設輸出 Ksav，或根據系統名稱輸出 Ksys 用以生成存儲資料增設輸出 Ksav，或，另外，保存於記錄再生器 300 之內部記憶體 307 內數據，與其他輸出到增設輸出做為存儲資料增設輸出 Ksav 使用也可。

在步驟 S 7 8 9，係在步驟 S 7 8 5 ~ S 7 8 8 其中之一藉由再生生成之存儲資料增設輸出 Ksav 保存增設輸出數據，並被容納於記錄裝置。

進而，在步驟 S 7 90，係步驟 S 7 8 2，S 7 8 3 中使設定之限制資訊被容納於資料管理檔案，資料管理檔案，係資訊形成圖 8 1 所示之格式，做為項目包含資料號碼、存儲信息識別子、記錄再生器識別子、程式使用限制、記錄再生器限制。

圖 8 2，係藉由圖 8 0 之處理用以再生，執行被容納於記錄裝置後之存儲資料增設輸出 Ksav，在步驟 S 7 9 1，係用以讀出執行程式之存儲信息識別子，記錄再生器限制

A 類式及通用中區資料標準 (CINEMA 規格 (210~207) 範圍) - 227 -

A7
B7

五、發明說明(225)

子，步驟 S 7 9 2 中，由圖 8 1 所示資料管理檔案用以讀出存儲信息識別子，記錄再生器識別子，程式使用限制，記錄再生器限制資訊，依情形，便程式使用限制以「假」使記錄再生器識別子不一致時，或使記錄再生器限制資訊以「假」使記錄再生器識別子不一致時，則進行終了處理。

其次，在步驟 S 7 9 3，S 7 9 4，S 7 9 5，係根據資料處理檔案之記錄資料將再生輸出生成處理設定於步驟 S 7 9 6 ~ S 7 9 9 之 4 態樣其中之一。

「有程式使用限制」且「有記錄再生限制」時，係在步驟 S 7 9 6 中，根據存儲信息間有輸出 (ex.Kcon)，及記錄再生器間有輸出 (Kdev) 雙方生成存儲資料增設輸出 Ksav，或，另外，保存於記錄再生器 300 之內部記憶體 307 內數據，與其他輸出到增設輸出做為存儲資料增設輸出 Ksav 使用也可，「有程式使用限制」且「無記錄再生限制」時，係在步驟 S 7 9 7 中，將存儲信息間有輸出 (ex.Kcon) 做為存儲資料增設輸出 Ksav，或根據存儲資料間有輸出 (ex.Kcon) 用以生成存儲資料增設輸出 Ksav，或，另外，保存於記錄再生器 300 之內部記憶體 307 內數據，與其他輸出到增設輸出做為存儲資料增設輸出 Ksav 使用也可。

「無程式使用限制」且「有記錄再生限制」時，係在步驟 S 7 9 8 中，將記錄再生器間有輸出 (Kdev) 做為存儲資料增設輸出 Ksav，或根據記錄再生器間有輸出 (

A 類式及通用中區資料標準 (CINEMA 規格 (210~207) 範圍) - 228 -

A7
B7

五、發明說明(226)

(Kdev) 用以生成存儲資料增設輸出 Ksav，或，另外，保存於記錄再生器 300 之內部記憶體 307 內數據，與其他輸出到增設輸出做為存儲資料增設輸出 Ksav 使用也可，並用「無程式使用限制」且「無記錄再生限制」時，係在步驟 S 7 9 9 中，系統共同輸出，譬如將系統名稱輸出 Ksys 做為存儲資料增設輸出 Ksav，或根據系統名稱輸出 Ksys 用以生成存儲資料增設輸出 Ksav，或，另外，保存於記錄再生器 300 之內部記憶體 307 內數據，與其他輸出到增設輸出做為存儲資料增設輸出 Ksav 使用也可。

此等之譯碼化輸出生成處理，係係適用對應於增設輸出生成處理之處理方法，根據同一之存儲信息間有輸出，記錄再生器間有輸出被譯碼化後之資料，依根據同一之存儲信息間有輸出，記錄再生器間有輸出藉由被生成之譯碼化輸出形成可譯碼化適用譯碼化輸出生成處理。

在步驟 S 8 00，係在上述步驟 S 7 9 6 ~ 7 9 9 其中之一使用被生成後之存儲資料譯碼化輸出被執行譯碼處理，並使譯碼存儲資料在記錄再生器 300 中被再生，執行。

若依據圖 8 0，8 2 中所示之存儲資料容納，再生處理流程，則被形成「進行程式使用限制」之選擇的存儲資料係由存儲信息間有輸出因為被執行譯碼化，譯碼化處理，所以持有同一存儲信息間有輸出被使用存儲信息資料進行譯碼化形成可進行利用，又，被形成「進行記錄再生器限制」之選擇的存儲資料，係藉由記錄再生器識別子

A 類式及通用中區資料標準 (CINEMA 規格 (210~207) 範圍) - 229 -

A7
B7

五、發明說明(227)

因為被執行譯碼化，譯碼化處理，所以持有同一記錄再生器識別子之記錄再生器，即藉由同一之記錄再生器進行譯碼化形成可進行利用。因此，藉由存儲信息，記錄再生器間有輸出可用以設定利用限制，形成可提昇存儲資料之安全性。

尚有，圖 8 0，圖 8 2 中，係顯示使用存儲信息間有輸出，記錄再生器間有輸出之存儲資料增設輸出，譯碼化輸出的生成處理，並使用存儲信息間有輸出之存儲信息間有輸出，又取代記錄再生器間有輸出之記錄再生器識別子，被此等識別子被用以執行存儲資料譯碼化輸出，譯碼化輸出之生成之構成也可。

其次，使用圖 8 3 ~ 8 5 項讓利用者之輸入的進行子對用以生成存儲資料之增設輸出，譯碼化輸出的構成加以說明。

圖 8 3 係根據利用者之輸入的進行子用以生成存儲資料之增設輸出被容納於記錄裝置之處理流程。

步驟 S 8 2 1，係由存儲信息資料讀出存儲信息識別子之處理，與前述各處理同樣，步驟 S 8 2 2，係藉由利用者用以決定是否進行程式使用限制之設定步驟，本構成中被設定之資料管理檔案，係資訊如有圖 8 4 所示之構成。

如圖 8 4 所示，資料，包含資料號碼，存儲信息識別子，記錄再生器識別子，選擇藉由利用者之程式使用限制資訊，「藉由利用者之程式使用限制資訊」係用以設定要

A 類式及通用中區資料標準 (CINEMA 規格 (210~207) 範圍) - 230 -

五、發明說明(228)

不要用以限制使用程式之利用者的項目。

在圖83中之處理流程之步驟8822的使用限制被形成設定，則步驟8823中被形成利用者通行字之輸入，並輸入，係譬如圖2所示由鍵盤等之輸入裝置被輸入，並輸入後之通行字，係在CPU106，控制部301之控制下被輸出到暗號處理部302，步驟8824中之處理，即根據輸入利用者通行字使存儲資料暗號化輸出Kiv被生成，被為存儲資料暗號化輸出Kiv，係譬如將通行字與暗號化輸出Kiv也可，或使利用記錄再生部之主輸出，藉由存儲資料暗號化輸出Kiv = DES (Mkx, 通行字) 進行生成也可，又，將通行字做為輸入用以適用一方向性函數，並根據該輸出用以生成暗號化輸出也可。

使步驟8822中之利用者限制被是No狀態時，則步驟8828中，根據記錄再生部300之系統共同暗號使存儲資料暗號化輸出被生成。

進而，在步驟8825以步驟8824，或步驟8828使用生成後之存儲資料暗號化輸出Kiv並使存儲資料暗號化處理被生成，步驟8826中使暗號化處理被生成後之存儲資料被收納於記錄被生成。

進而，步驟8827中，在圖84之資料管理畫面以步驟8822藉由設定後之利用者使用限制使用限制資訊，被資訊附於存儲資訊識別子及記錄再生部識別子。

圖85係顯示藉由圖83之處理流程被收納後之存儲資

五、發明說明(229)

料之再生處理被生成，步驟8831中，由存儲資訊資料選出存儲資訊識別子，並在步驟8832中由圖84所示之資料管理畫面選出存儲資訊識別子，藉由利用者選擇形式使用限制資訊。

步驟8833中，根據資料管理畫面中之資料用以執行判定，使「藉由利用者通行字形式使用限制」被設定時，則步驟8834中，求出通行字輸入，步驟8835中，根據輸入通行字用以生成暗號化輸出，該暗號化輸出被生成後，係根據利用暗號化輸出被生成後之處理被生成，根據通行字被暗號化後之資料，係根據同一之通行字經由該生成後之暗號化輸出被生成可暗號化被設定於暗號化輸出被生成。

使步驟8833之判定藉由利用者通行字形式使用限制時，則步驟8837中按字節於記錄再生部300之內部記憶體的系統共同暗號，譬如使用系統暗號Kiv，使存儲資料暗號化輸出Kiv被生成，或，另外，保存於記錄再生部300之內部記憶體307內放置，與其他暗號化輸出之暗號化輸出被存儲資料暗號化輸出Kiv使用也可。

在步驟8836，係步驟8835，步驟8837其中之一中使用從生成後之暗號化輸出Kiv使被收納於記錄被生成後之存儲資料之暗號化輸出，並在步驟8836之記錄再生部中被形成存儲資料之再生，執行。

若依據圖83，85中所示之存儲資料資訊，再生處理被生成，則被形成「藉由利用者通行字形式使用限制」之

五、發明說明(230)

選擇的存儲資料係因為藉由根據利用者輸入通行字的暗號化輸出被暗號化處理，所以被輸入同一通行字時進行暗號化處理可適用，可成為提高存儲資料之安全性。

以上，對於無誤之存儲資料收納處理，再生處理被生成說明，但將上述之處理進行組合後之處理，譬如將通行字，記錄再生部識別子，存儲資訊識別子等任意組合運用用以生成存儲資料暗號化輸出，暗號化輸出之生成也可。

(17) 不正當復舊之排除(Revocation)構成

如已經說明，本發明之資料處理裝置中，由該圖500(參照圖3)，通訊裝置600將被提供之復舊的存儲資訊資料在記錄再生部300中，用以執行暗號化處理等，藉由收納於記錄裝置之構成而使提供存儲資訊之安全性，同時又，使使正當利用者持有可利用之構成。

由上述之說明能理解，輸入存儲資訊，係使被收納於記錄再生部300之暗號化處理部302被收納於內部記憶體307之復舊的暗號化輸出，主輸出，該暗號化輸出被暗號化(參照圖18)，使暗號化處理，暗號化處理，暗號化處理被生成，用以收納該暗號化資訊之內部記憶體307，係如前面已說明，基本上被構成由外部設有暗號化處理的半導體晶片，具有多種構造，除其內部記憶體被保護於記錄部之裝置，或被構成於如下圖，又，使動作之電腦裝

五、發明說明(231)

且頻率之復舊等等，被構成使為由外部難以不正當資料之選出的特徵被構成，但為一使內部記憶體之不正當復舊被執行，使此等之暗號化資訊等被選出，在來有正規許可證之記錄再生部被限制，藉由被限制後之暗號化資訊而不正當的存儲資訊利用有可能被形成。

於此，由於此等之不正當復舊藉由暗號化之限制對於用以防止存儲資訊之不正當利用的構成加以說明。

圖86係顯示用以說明本構成「(17) 不正當復舊之排除構成」方塊圖，記錄再生部300，係如圖2、圖3所示記錄再生部構成，具有內部記憶體，而圖86係圖(18)各種之暗號化資訊，進而，具有記錄再生部識別子，與有，於此，係藉由第三者被限制之記錄再生部識別子，暗號化資訊等係不直接收納於圖3所示內部記憶體307，圖86所示記錄再生部300之暗號化資訊等，係藉由暗號化處理部302(參照圖2、3)在可存貯的記錄部裝置，或進行分散被收納於構成。

為了用以實現不正當復舊之排除構成，欲用以記錄存儲資訊資料後之裝置部的不正當記錄再生部識別子名單之構成，如圖86所示，在存儲資訊資料，係由不正當之記錄再生部識別子(IDrev)名單用以有復舊排除(Revocation)名單，進而，設有排除名單之復舊排除利用之名單被限制ICVrev，不正當之記錄再生部識別子(IDsav)名單，係使存儲資訊提供者，或管理時，譬如由不正當復舊之復舊排除利用後之不正當記錄再生部識別子IDrev延

A7
B7

五、發明說明(232)

行名單化等，該排除名單係暫留而由配接端 Kdis 被刪除後再進行存納也可，藉由記錄再生器對於該排除名單，係暫留而圖 22 之存儲信息下載處理之狀態圖樣。

尚有，前述，為了容易理解，將排除名單做為單獨之資料顯示於圖 86 之存儲信息資料中，但譬如在前圖已說明之存儲信息資料之集羣部的構成要素之處理方針（譬如參照圖 32~35）中其含排除名單也可，該情形，係藉由前圖已說明之核對值 ICVA 含排除名單處理方針資料之寫改後對形成，並排除名單適合於處理方針中時，係藉由核對值 A：ICVA 之排除名單替代，並記錄於再生器內之核對值 A 生成端 Kicv 被利用，而不必要用以前圖核對值生成端 Kicv-rev。

將排除做為單獨之資料並基於存儲信息資料中時，藉由排除之寫改後對用名單核對值 ICVrev 用以執行排除之核對，同時由名單核對值 ICVrev 及存儲信息資料中之其他部分核對值用以生成中核對值並進而進行中間核對值之驗證處理的構成。

藉由排除之寫改後對用名單核對值 ICVrev 的排除名單之核對方法，係與前述圖 23、圖 24 已說明之 ICVA、ICVB 等核對值生成處理以同樣之方法可執行，即，將保存於記錄再生器端就處理部 302 之內部記憶部 307 後之核對值生成端 Kicv-rev 做為端點，並將該適合於存儲信息資料之排除名單就其信息從圖 23、圖 24 已說明之 ICV 計算方法被計算，用以比較計算後之核對

A. 核對值生成用中間數據表 (CNSIM 規格 103~207 公案) - 235 -

A7
B7

五、發明說明(233)

值 ICV-rev⁽²³³⁾ 及被容納於集羣 (Header) 內後之核對值：ICV-rev，在進行一致後時，則進行判定異常處理。

含名單核對值 ICVrev 之中間核對值，係譬如，如圖 25 所示，將被保存於記錄再生器端就處理部 302 之內部記憶部 307 的核對值生成端 Kicv 做為端點，並在驗證後之 Header 內之核對值 A、核對值 B、名單核對值 ICVrev，進而根據格式加上存儲信息核對值後之信息利用以前圖 7 其餘已說明之 ICV 計算方法進行生成。

此等之排除名單，名單核對值，係通過 DVD、CD 等之媒體 500，透過裝置 600，或透過記憶卡等之記錄裝置 400 並被提供對記錄再生器 300，於此記錄再生器 300，係保有正常的端點之記錄再生器時，則會有與不正寫複製之識別于 ID 的情形。

圖 87 及圖 88 係顯示如此構成中之不正當的記錄再生器之排除處理的處理流程圖，圖 87 係由 DVD、CD 等之媒體 500，或透過裝置 600 被提供存儲信息時之不正當記錄再生器排除 (Revocation) 處理流程圖，圖 88 係由記憶卡等之記錄裝置 400 被提供存儲信息時之不正當記錄再生器排除 (Revocation) 處理流程圖。

首先，對於圖 87 之處理流程加以說明，步驟 S901，係用以與舊核對值，存儲信息之提供，即進行再生處理或下載等步驟，該圖 87 所示之處理，係譬如在記錄再生器端就處理部 302 內之媒體並被採用以執行下

A. 核對值生成用中間數據表 (CNSIM 規格 103~207 公案) - 236 -

A7
B7

五、發明說明(234)

載處理等之步驟的步驟被執行，對於下載處理，係使用如前圖 22 之說明，做為圖 22 之處理流程的執行前步驟，或做為被納入於圖 22 之處理流程中的處理便於圖 87 之處被執行。

處理部再生器 300 透過通訊部之通訊裝置接收存儲信息提供時，係用以與前圖 87 內之存儲信息是記錄值核對的通訊對照時間，之後，進而步驟 S902。

在步驟 S902，係由存儲信息資料之集羣部用以取得排除名單 (參照圖 86)。該名單取得處理，係在再生器內有存儲信息時，則基於圖 3 所示控制部 301 通過通訊部 304 由通訊裝置進行，而由通訊裝置有存儲信息時，則後圖 3 所示控制部 301 通過通訊部 305 由存儲信息是記錄值被接收。

其次步驟 S903 中，控制部 301，係在記錄再生器端就處理部 302 由媒體 500 或透過裝置 600 將記錄後之排除名單再轉交到記錄再生器端就處理部 302，並被執行核對值生成處理，記錄再生器 300，係在內部基於排除核對值生成端 Kicv-rev，將接收後之排除名單就其信息用以適用排除核對值生成端 Kicv-rev，譬如依圖 23、圖 24 已說明之 ICV 計算方法用以計算核對值 ICV-rev⁽²³⁴⁾，並用以比較計算結果及被容納於存儲信息資料之 (Header) 內之核對值：ICV-rev，在進行一致後則判定無異常 (在步驟 S904 Yes)，未一致時，則被判定有異常，並進而步驟 S909

A. 核對值生成用中間數據表 (CNSIM 規格 103~207 公案) - 237 -

A7
B7

五、發明說明(235)

將處理流程進行了處理。

其次，步驟 S905 中，記錄再生器端就處理部 302 之控制部 306，係在記錄再生器端就處理部 302 之端點 / 譯碼化部 308 被提供核對值 ICVT⁽²³⁵⁾ 之計算，根據核對值 ICVT，係如圖 25 所示，將被保存於記錄再生器端就處理部 302 之內部記憶部 307 的系統名稱 Ksys 做為端點，將中間核對值以 DVD 進行核對值加以生成，尚有，各部分核對值，譬如 ICVA、ICVB 等之驗證處理，係在該圖 87 所示處理流程中係省略，但前圖已說明之圖 39~圖 45 之處理流程同樣係進行根據各資料格式之部分核對值的驗證。

其次，步驟 S906 中，用以比較生成後之核對值 ICVT⁽²³⁵⁾ 及集羣 (Header) 內之 ICVT，在進行一致後時 (在步驟 S906 Yes)，則進到步驟 S907，未一致時，則被判定有異常，並進到步驟 S909 做為異常處理進行了處理。

如前圖已說明，根據核對值 ICVT，係 ICVA、ICVB，進而，根據資料格式之存儲信息系統之核對值等，將被適合於存儲信息資料之部分核對值系統進行核對，但於此，在此等之部分核對值應用，將排除名單之寫改後對用名單核對值 ICVrev 做為各部分核對值之外，用以驗證此等全部之寫改，藉由上述處理從生成後之核對值與被容納於集羣 (Header) 內之核對值：ICVT 進行一致後時，則被判斷 ICVA、ICVB，各存儲信息系統之

A. 核對值生成用中間數據表 (CNSIM 規格 103~207 公案) - 238 -

五、發明說明(236)

核對部，及名單核對部 ICVrev全部無更改。

進而，在步驟 S907，係根據形成用以比較被判定無更改之除除名單，及被寄附於自己之記錄再生器 300 後之記錄再生器識別子 (IDdev)。

由於存儲係在資料在被讀出後之不正當的記錄再生器識別子 IDdev 之名單裡含有自己之記錄再生器之識別子 IDdev 時，則該記錄再生器 300，係被判定具有不正當被複製之輪胎資料，並進到步驟 S909，以後之手續係被中止。譬如，做為不能執行圖 22 之存儲信息下載處理之手段。

步驟 S907 中，在不正當之記錄再生器識別子 IDdev 之名單裡判定未含有自己之記錄再生器之識別子 IDdev 時，則該記錄再生器 300，係被判定具有正當的輪胎資料，並進到步驟 S908，以後之手段。譬如，程式執行處理，或形成可執行圖 22 等之存儲信息下載處理等。

圖 88 係顯示用以再生車輛於記憶卡等之記錄裝置 400 缺之存儲信息資料的處理，如圖 88 說明，記憶卡等之記錄裝置 400 及記錄再生器 300，係使圖 20 缺之相互認證處理 (步驟 S921) 被執行。步驟 S922 中，係在相互認證 OK 時，進到步驟 S923 以後之處理，相互認證失敗時，則形成步驟 S930 之輪胎。以後之處理係不實施執行。

在步驟 S923，係由存儲信息資料之無管理用以取捨排除名單 (參考圖 36)，以後步驟 S924。

本報係以通稱中韓語譯本 (CNDA 規格 2007-297 公案) - 249 -

本報係以通稱中韓語譯本 (CNDA 規格 2007-297 公案) - 249 -

五、發明說明(237)

S930 之處理，係與前面圖 87 中之對應處理同樣之處理，即，藉由名單核對部之名單驗證 (S924)。

S925，藉由該驗證之驗證 (S926、S927)，用以執行比較 (S928) 名單之項目及自己之記錄再生器識別子 IDdev，並由存儲信息資料在被讀出後之不正當的記錄再生器識別子 IDdev 之名單裡含有自己之記錄再生器之識別子 IDdev 時，則該記錄再生器 300，係被判定具有不正當被複製之輪胎資料，並進到步驟 S930，被中止以後之手段。譬如，做為不能執行圖 28 所示等儲信息之再生處理。另外，在不正當之記錄再生器識別子 IDdev 之名單裡判定未含有自己之記錄再生器之識別子 IDdev 時，則該記錄再生器 300，係被判定具有正當之輪胎資料，並進到步驟 S929，形成可執行以後之手段。

如此，本發明之資料處理裝置中，係使存儲信息提供者，或管理者提供之存儲信息一起用以識別不正當的記錄再生器之資料，即將不正當之記錄再生器識別子 IDdev 進行名單化或將排除名單做為存儲信息資料之無管理之輪胎資料一起提供到存儲信息利用者。而記錄再生器利用者，係藉由記錄再生器在存儲信息的利用之前，用以執行核對等寄附於自己之記錄再生器之記憶體後之記錄再生器識別子 IDdev，及名單之識別子並做進行一致之資料存在時，則做為不能執行以後之處理所以用以限制輪胎資料並藉由寄附於記憶體後之不正當的記錄再生器形成用以排除存儲信息利用。

本報係以通稱中韓語譯本 (CNDA 規格 2007-297 公案) - 249 -

本報係以通稱中韓語譯本 (CNDA 規格 2007-297 公案) - 249 -

五、發明說明(238)

(18) 安全晶片構成及製造方法

如前文已說明，記錄再生器端部處理部 302 之內部記憶體 307，或記錄裝置 400 之內部記憶體 405，係再用以保持秘密性無恥等之重要的資訊，所以由外部有必須形成或具有不正當讀出之構造。因此，記錄再生器端部處理部 302，記錄裝置端部處理部 401，係譬如被構成由外部持有者以存取構造的中間體晶片，具有多層構造，而其內部之記憶體係被保持於記憶等之狀態，或被構成由讀下層，又，使動作之狀態或／且頻率之更改等等，並構成與新式記憶體具有由外部讀出以不正當資料讀出的特性。

可是，在上述之說明能被理解，譬如記在記錄再生器端部處理部 302 之內部記憶體 307 係在記錄再生器名稱 Kdev 等之各記錄再生器形成必要寫入不同的資料。又，晶片內之非易失性的記憶領域，譬如在閃光記憶體，F e R A M 等各晶片之記憶資訊，譬如寫入識別資訊 (ID) 或輪胎輪胎資料後，譬如在製品出產後將資料之再入，讀出必要形成困難。

譬如技術之有資料的讀出，為了將再寫入處理後為困難之方法，係譬如將資料寫入之指令通訊協議編碼部。即，接受晶片上之資料寫入指令的信號，及在製品化之使用以分離被利用通訊用的信號被之構成，在該晶片上直接送這信號將資料寫入指令不會形成有效等之

本報係以通稱中韓語譯本 (CNDA 規格 2007-297 公案) - 249 -

本報係以通稱中韓語譯本 (CNDA 規格 2007-297 公案) - 249 -

五、發明說明(239)

方法。

可是，即使採用如此之譬如技術方法，對於具有記憶元件之專門知識者而言，亦可使輪胎輪胎之讀取及技術，則對晶片之資料寫入區域可僅讀輸出，又，即使資料寫入之指令通訊協議編碼部，但通訊協議之解析可被性係經常存在。

如此，將用以保持秘密性資料之可改變的輪胎輪胎資料之存貯元件使成流過，係形成輪胎輪胎或現系統全體之結果，又，為了用以防止資料之讀出，也可做為不實資料讀出而令輪胎之輪胎，係該情形，即使用以執行正統之資料寫入時，對記憶體使資料寫入用以確認是否實際進行，該被寫入後之資料形成不能用以判定是否正確被寫入，僅進行可將資料寫入之晶片可產生被快給。

有鑑於此等之譬如技術，因此，提供一種安全晶片構成及安全晶片製造方法，在 F e R A M 等非易失性記憶體為可正確之資料寫入，同時將資料之讀出形成困難。

圖 89 係顯示譬如可適用於前述之記錄再生器端部處理部 302 或記錄裝置 400 之輪胎輪胎部 401 的安全晶片構成。圖 89 (A) 係顯示晶片之製造過程，即，原料之寫入過程中之安全晶片構成。圖 89 (B) 係顯示用以將新寫入資料後之安全晶片之製品構成，即，記錄再生器 300，記錄裝置 400 之例。

製造過程中之安全晶片，係在處理部 8001 使模型製造用信號晶片 303，及在模指令信號線 8004 被製造

本報係以通稱中韓語譯本 (CNDA 規格 2007-297 公案) - 249 -

本報係以通稱中韓語譯本 (CNDA 規格 2007-297 公案) - 249 -

五、發明說明 (240)

據，處理部 8001，係以模式指定用信號線 8003 讀取設定後之模式，譬如根據資料寫入模式或資料讀出模式對非易失性記憶體之記憶部 8002 之資料寫入處理，或由記憶部 8002 用以執行資料讀出處理。

另外，圖 89(B)之安全晶片所搭載部品中，係使安全晶片及外部連接接口、周邊電路、其他元件等以汎用信號線連接，但模式信號線 8003，係並非連接狀部，具體性的處理，係譬如將模式指定用信號線 8003 進行接地連接，用於 Vcc，用以切斷信號線，或以絕緣體層進行外封等。藉由如此處理，製品出廠前，係對安全晶片之模式信號線使用形成阻斷，由外部部品片之資料讀出或寫入可確保可靠性。

進而，本構成之安全晶片 8000，係持有對資料之記憶部 8002 寫入處理，及被寫入於記憶部 8002 後之資料讀出處理形成阻斷之構成，即便第三者在模式信號線 8003 之存取進行成功時也可防止不正當的資料寫入、讀出。圖 90 係顯示具有本構成之安全晶片中之資料寫入或讀出處理流程圖。

步驟 S951，係將模式信號線 8003 設定成資料寫入模式或資料讀出模式之步驟。

步驟 S952，係當晶片取出認證用資訊的步驟，本構成之安全晶片，係譬如藉由電線 (Wire)，與 ROM 構成，預先在進行中，將該技術中之認證用的鑰匙資訊等，在認證處理後等納必要的資訊，步驟 S952，係用以

五、發明說明 (241)

讀出該部認證資訊並用以執行部認證處理，譬如將正確的資料寫入型號，資料讀出裝置連接於汎用信號線用以執行認證處理時，則取該認證 OK (步驟 S953 中之 Yes) 之結果，但將不正當的資料寫入型號，資料讀出裝置連接於汎用信號線用以執行認證處理時，則認證失敗 (步驟 S953 中之 No)，並在該時將認證處理中止，認證處理，係譬如依據該前面已說明之圖 13 的相互認證處理手續可執行。圖 89 所示之處理部 8001，係具有可執行此等之認證處理的構成，此係，譬如藉由前面已說明之圖 29 所示並與於認證部 400 之信號處理部 401 的控制部 403 後之指令寄存器等部之構成可實現，譬如圖 89 之晶片處理部，係持有與圖 29 所示並與於認證部 400 之信號處理部 401 的控制部 403 後之指令寄存器等部之構成，係由連接於各指令信號線 8004 後之機器使用之指令 No 被輸入，則用以執行對應之處理，並可形成用以執行認證處理程序。

處理部 8001 係認證處理中係根據形成部認證，接受資料之寫入指令，或資料之讀出指令用以執行資料之寫入處理 (步驟 S955)，或資料之讀出處理 (步驟 S956)。

如此本構成之安全晶片，係在資料之寫入時，讀出時係與用以執行認證處理的構成，所以由於未持有正當權限之第三者由安全晶片之記憶部可用以防止資料之讀出，或寫入到記憶部。

五、發明說明 (242)

其次，進而，圖 91 係顯示係安全性能之元件構成的實施例圖。在該例，係使安全晶片之記憶部 8002 被分成 2 個領域，一方面係可資料讀寫的讀出專用領域 (R: Read Write 領域) 8201，而另一方面係可資料寫入之寫入專用領域 (W: Write Only 領域) 8202。

該構成中，在寫入專用領域 (W: Write Only 領域) 8202，係存入除鑰匙資訊外，諸如子資訊等要求高安全性的資料，而一方之安全性能較低者，譬如將技術用之資料等寫入讀出專用領域 (R: Read Write 領域) 8201。

處理部 8001，係由讀出專用領域 (R: Read Write 領域) 8201 之資料讀出處理，係根據前述之圖 30 說明之認證處理用以執行資料讀出處理，可是，資料寫入處理，係依據圖 92 之流程進行執行。

圖 92 之步驟 S961，係將模式信號線 8003 設定成寫入模式之步驟，在步驟 S962，係用以執行圖 89 已說明認證的認證處理，在認證處理後形成認證，則進到步驟 S963，透過指令信號線 8004，在寫入專用 (W) 領域 8202 寫入安全性的鑰匙資訊等資訊，在讀出專用領域 (R: Read Write 領域) 8201 係讀出該鑰匙資訊的，譬如將該處理用資料寫入於對照部 8001 進行輸出。

在步驟 S964 係根據受指令後之處理部 8001，將該指令中之資料寫入處理分別於寫入專用 (W) 領域

五、發明說明 (243)

8202，讀出寫入專用領域 (R: Read Write 領域) 8201 進行執行。

又，圖 93 係顯示係寫入於寫入專用 (W) 領域 8201 後之資料的認證處理流程圖。

圖 93 之步驟 S971，係與圖 8001 中，根據輸入於寫入專用 (W) 領域 8202 後之資料係根據處理執行，此等之執行流程，係與前面之認證處理執行流程同樣，將該部認證指令寄存器等部之信號處理程序藉由順序執行之構成被實現，又，處理部中之鑰匙資訊的處理係與前部被實現，譬如可與前用以執行前部已說明之 DES 算法的構成。

其次，在步驟 S972，係根據連接於安全晶片後之驗證資訊由處理部 8001 用以取得驗證處理結果，接著，步驟 S973 中，在該部認證部對進行寫入處理後之正確的寫入資料在處理部 8001 中執行該之算法及適用同樣之鑰匙化處理取得之結果，由處理部 8001 用以比較認證化結果。

彼此比較之結果若有一致，則將寫入於寫入專用 (W) 8202 後之資料係驗證正確。

在該構成，係根據認證處理後取得並發出指令寫入形成可執行，但資料之可讀出處理，係係限定於讀出專用領域 (R: Read Write 領域) 8201，而將寫入於寫入專用 (W) 領域 8202 後之資料讀出，係不可能，進而形成高的安全性的構成，又，與完全為不能讀出之

A7
B7

五、發明說明(244)

品片不同，被讀或有讀出入存到個域（只寫：Read Write 領域）8 2 0 1 所以從記憶體是否正確可被對。

以上，一方面參考特定之實施例，一方面對於本發明做了詳解，可是，在不脫離本發明之要旨的範圍內業者可修正或代用該實施例係自知之明，即，在所需例示之形態將本發明做了揭示，所以不應應定性的被解釋，又，在上述之實施例係保存信息之記錄，可再生之記錄再生器做為例做了說明，但僅可資料記錄，僅可資料再生之裝置中也可適用本發明之構成，本發明係個人電腦、遊戲機器、一般其他各種資料處理裝置中可實施，為了用以判斷本發明之要旨，應參考記載於最後之專利申請範圍。

【發明之效果】

如此，若依據本發明之資料處理裝置及資料處理方法，則將存儲信息資料分割成複數部分之部分資料對合 1 以上部分資料集合做為複數個值並由被生成之部分核對值之核對處理用以執行部分資料之驗證處理，並將部分核對值對該數個值合後之部分核對值集合進行驗證處理由部分核對值驗證處理對值之核對處理，將用於用以將該部分核對值集合之複數的部分核對值對該數之部分資料集合全應用以執行驗證處理做為構成，所以對於存儲信息資料全體與該步驟一之核對值之構成不同，形成可部分之驗證處理，又，全體之驗證處理，或使部分核對值對該值進行執行，所以可既有效。

本國式及適用中國國家標準 (CNS)A 規格 (210×287 公釐) - 247 -

A7
B7

五、發明說明(245)

進而，若依據本發明之資料處理裝置及資料處理方法，則對無更改之處的資料部分予以省略驗證處理等，存儲信息資料之使用態樣，譬如根據下載或，再生處理形成可驗證處理，可進行依據使用根據之有效的驗證。

進而，若依據本發明之資料處理裝置及資料處理方法，則為了用以執行資料暗號化，資料暗號化，資料認證，認證處理，等名稱處理等之暗號化處理時形成必要的個別驗證點不用寄附於記錄部，為了用以生成此等之個別驗證點持有再生主驗證點寄附於記錄部之構成，使資料處理裝置中之驗證處理部，將暗號化，認證處理等之暗號化處理時形成必要的個別驗證點，將對應於此等之個別驗證點的主驗證點由記錄部取出，併集現出之主驗證點，及與該資料之個別驗證點，譬如用以執行通用 DES 算法之暗號化處理，做為用以生成暗號化驗證點，認證處理等之個別驗證點之構成，所以使個別驗證點皆由記錄部不會改變，為了取得個別驗證點，係個別驗證點生成算法，及主驗證點之雙方資訊，進而與該資料之個別驗證點，使該驗證點資訊形成必要，從而可提昇暗號化處理系統之安全性，又，使個別驗證點由於任何理由而失效時，但其被寄附驗證點因被限定於個別驗證點之範圍，所以可對系統全體無影響。

進而，若依據本發明之資料處理裝置及資料處理方法，則根據與該資料之個別驗證點，用以以逐次生成個別驗證點，所以將適用於各台之裝置的驗證點名單在管理裝置不必加以保持，形成提高安全性及降低容易系統管理。

本國式及適用中國國家標準 (CNS)A 規格 (210×287 公釐) - 248 -

A7
B7

五、發明說明(246)

進而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料生成方法，則在存儲信息資料用以寄附於不正當機構之個別資料資訊，並在記錄再生器中之存儲信息利用之前，用以執行不正當機構，及取利用存儲信息之記錄再生器將記錄再生器對該子之核對處理，核對結果，在含於不正當機構名單之項目與記錄再生器對該子使進行一致項目存在時，則以後之處理，譬如被刪除以中止存儲信息資料讀取，下載，再生處理等之執行則構成可藉由不正當取得後之再生機構等形成可用以排除存儲信息的不正當利用。

進而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料生成方法，則被讀取存儲信息資料中之不正當機構名單用之核對值集合併合於存儲信息資料之構成，所以可造成防止名單自體之篡改，進而成為可提供高安全性的存儲信息資料利用構成。

進而，若依據本發明之資料處理裝置及資料處理方法，則在記錄再生器，P C 等之資料處理裝置用以寄附資料處理裝置內有之驗證點有驗證點，及在用以利用存儲信息資料之其他資料處理裝置用以寄附於共同系統驗證點則以根據存儲信息之利用限制形成可存儲信息處理，資料處理裝置，保持此等之驗證點則以根據信息之利用限制以選擇性加以利用，譬如在該資料處理裝置中有可利用之存儲信息時，則使用資料處理裝置內有之驗證點，另外，在其他之系統中也可利用存儲信息時則使用系統共設共同驗證點執行存儲

本國式及適用中國國家標準 (CNS)A 規格 (210×287 公釐) - 249 -

A7
B7

五、發明說明(247)

信息資料之核對值生成，核對處理，僅在進行核對成立時用以暗號化資料形成可進行再生，所以使資料處理裝置可利用存儲信息，或在本系統進行共同利用之存儲信息等，形成可根據存儲信息之利用限制之處理。

進而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料驗證賦予方法，則在存儲信息區段資料單位用以生成存儲信息核對值，並用以執行生成後之存儲信息核對值之核對處理，進而，根據驗證對合之存儲信息區段資料用以生成存儲信息中間值並由通用存儲信息核對值生成驗證點之驗證處理做為生成存儲信息核對值之構成，所以比之譬如技術之資料全體之處理可形成有效的驗證。

進而，若依據本發明之資料處理裝置，資料處理方法及存儲信息資料驗證賦予方法，則在存儲信息區段資料單位可驗證，同時存儲信息資料之使用態樣，譬如可形成根據下載處理，再生處理之暗號化的驗證處理，可進行依據使用根據之有效的驗證。

進而，本發明之資料處理裝置，存儲信息資料生成方法，及資料處理方法中，係在存儲信息資料中設有複數之存儲信息區段，在各存儲信息區段單位持有可被寫入暗號化處理之構成，又將使用信息暗號化之驗證點進而進行暗號化做為暗號化於該區段之構成，所以譬如使該區段之存儲信息區段存在，並使暗號化處理之必要的區段，及不要的區段進行生成，也可形成做為用以以該區段發後之任意的資料構成。

本國式及適用中國國家標準 (CNS)A 規格 (210×287 公釐) - 250 -

五、發明說明(240)

進而，若依據本發明之資料處理裝置、資料處理系統、及資料處理方法，則將存儲信息區段之構成持有規則性的構成，譬如持有一排之資料片之構成，或藉由像以文書用以配置階梯化區段及非階梯化（平書文）區段的構成，形成可快速用以執行其譯碼處理，根據存儲信息資料之內容的選擇，譬如可形成適用於將資料之再生等的階梯化存儲信息資料之提供。

進而，本發明之資料處理裝置、資料處理方法及存儲信息資料生成方法，係使存儲信息可有效地執行被壓縮後之聲音資料，或有聲音資料等情形之再生處理，即，將存儲信息資料之構成與綜合解碼資料及伸長處理程式之構成，在再生處理裝置中，形成可適用附帶於壓縮存儲信息資料之伸長處理程式的伸長處理，在再生處理裝置內使伸長處理程式不存在可避免不能再生之事態。

進而，若依據本發明之資料處理裝置、資料處理方法及存儲信息資料生成方法，則將存儲信息資料之構成與像以容納解碼資料及其壓縮處理程式與解碼後之聲音部的組合，又，使存儲信息有伸長處理程式時，將存儲信息資料藉由以容納伸長處理程式及其程式擴展後聲音部之組合，使再生處理裝置將可適用於壓縮存儲信息資料的伸長處理程式根據聲音部執行判定，進而將再生處理裝置由可存取之記錄裝置等用以檢索可適用的程式做為用以執行伸長處理之構成，所以藉由利用該形態不必用以執行程式擴展處理，可形成有效的再生處理。

本國際式專利申請中譯國語版本 (CNS144 規格 (116+207 字數)) - 251 -

五、發明說明(240)

【圖式之簡單說明】

- 圖 1 係顯示本發明之資料處理系統的構成圖。
- 圖 2 係顯示本發明裝置採用資料處理裝置之構成圖。
- 圖 3 係顯示本發明裝置採用資料處理裝置之構成圖。
- 圖 4 係顯示在媒體上，通訊路上之存儲信息資料的資料格式圖。
- 圖 5 係顯示被包含於存儲信息資料中之聲音的處理方法圖。
- 圖 6 係顯示被包含於存儲信息資料中之聲音資訊圖。
- 圖 7 係顯示使用 D E S 之電子署名生成方法圖。
- 圖 8 係顯示使用三倍 D E S 之電子署名生成方法圖。
- 圖 9 係用以說明三倍 D E S 之整體圖。
- 圖 10 係顯示在一部分使用三倍 D E S 之電子署名生成方法圖。
- 圖 11 係顯示電子署名生成中之處理流程圖。
- 圖 12 係顯示電子署名生成中之處理流程圖。
- 圖 13 係用以說明使用對稱鑰匙技術之相互認證處理之處理程序圖。
- 圖 14 係用以說明公開鑰匙證明書圖。
- 圖 15 係用以說明使用非對稱鑰匙技術之相互認證處理之處理程序圖。
- 圖 16 係顯示使用獨有曲線帶時之階梯化處理的處理流程圖。

本國際式專利申請中譯國語版本 (CNS144 規格 (116+207 字數)) - 252 -

五、發明說明(250)

圖 17 係顯示使用獨有曲線帶時之階梯化處理的處理流程圖。

圖 18 係顯示記錄再生時上之資料保持狀態圖。

圖 19 係顯示記錄裝置上之資料保持狀態圖。

圖 20 係顯示記錄再生時及記錄裝置之相互認證處理流程圖。

圖 21 係顯示記錄再生時之主鑰匙及記錄裝置之對稱鑰匙區段的關係圖。

圖 22 係顯示存儲信息之下載處理中的處理流程圖。

圖 23 係用以說明核對值 A：I C V a 之生成方法圖。

圖 24 係用以說明核對值 B：I C V b 之生成方法圖。

圖 25 係用以說明核對數，記錄再生裝置有核對值之生成方法圖。

圖 26 係顯示被保存於記錄裝置之存儲信息資料的格式（利用限制資訊 = 0）圖。

圖 27 係顯示被保存於記錄裝置之存儲信息資料的格式（利用限制資訊 = 1）圖。

圖 28 係顯示存儲信息之再生處理中的處理流程圖。

圖 29 係對於記錄裝置中之指令執行方法說明圖。

圖 30 係對於記錄裝置中之存儲信息存取處理的指令執行方法說明圖。

圖 31 係對於記錄裝置中之存儲信息再生處理的指令

本國際式專利申請中譯國語版本 (CNS144 規格 (116+207 字數)) - 253 -

五、發明說明(251)

執行方法說明圖。

- 圖 32 係用以說明存儲信息資料格式之格式形態 0 的構成圖。
- 圖 33 係用以說明存儲信息資料格式之格式形態 1 的構成圖。
- 圖 34 係用以說明存儲信息資料格式之格式形態 2 的構成圖。
- 圖 35 係用以說明存儲信息資料格式之格式形態 3 的構成圖。
- 圖 36 係用以說明格式形態 0 中之存儲信息核對值 I C V i 的生成處理方法圖。
- 圖 37 係用以說明格式形態 1 中之存儲信息核對值 I C V i 的生成處理方法圖。
- 圖 38 係用以說明格式形態 2、3 中之核對值，記錄再生裝置有核對值之生成處理方法圖。
- 圖 39 係顯示格式形態 0、1 中之存儲信息下載處理的處理流程圖。
- 圖 40 係顯示格式形態 2 中之存儲信息下載處理的處理流程圖。
- 圖 41 係顯示格式形態 3 中之存儲信息下載處理的處理流程圖。
- 圖 42 係顯示格式形態 0 中之存儲信息再生處理的處理流程圖。
- 圖 43 係顯示格式形態 1 中之存儲信息再生處理的處理

本國際式專利申請中譯國語版本 (CNS144 規格 (116+207 字數)) - 254 -

五、發明說明 (252)

種說明書。

圖 4 4 係顯示格式形態 2 中之存儲信息再生處理的處理流程圖。

圖 4 5 係顯示格式形態 3 中之存儲信息再生處理的處理流程圖。

圖 4 6 係用以說明存儲信息生成者，及存儲信息驗證者中之核對值的生成、驗證方法圖 (其 1)。

圖 4 7 係用以說明存儲信息生成者，及存儲信息驗證者中之核對值的生成、驗證方法圖 (其 2)。

圖 4 8 係用以說明存儲信息生成者，及存儲信息驗證者中之核對值的生成、驗證方法圖 (其 3)。

圖 4 9 係對於使用主鑰匙將各種鑰匙以個別生成之方法說明圖。

圖 5 0 係顯示對於使用主鑰匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖 (例 1)。

圖 5 1 係顯示對於使用主鑰匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖 (例 2)。

圖 5 2 係用以說明藉由主鑰匙之分開使用，對於用以執行利用限制之構成圖。

圖 5 3 係顯示對於使用主鑰匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖 (例 3)。

本說明書所載之圖式係以簡化之圖式表示。

五、發明說明 (253)

圖 5 4 係顯示對於使用主鑰匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖 (例 4)。

圖 5 5 係顯示對於使用主鑰匙將各種鑰匙以個別生成之方法，存儲信息提供者，及利用者中之處理例圖 (例 5)。

圖 5 6 係顯示將通用三合 DES 之暗鑰匙使用單 DES 算法進行容納處理流程圖。

圖 5 7 係顯示根據優先順位之存儲信息再生處理流程 (例 1) 圖。

圖 5 8 係顯示根據優先順位之存儲信息再生處理流程 (例 2) 圖。

圖 5 9 係顯示根據優先順位之存儲信息再生處理流程 (例 3) 圖。

圖 6 0 係用以說明對於用以執行存儲信息再生處理中之壓縮資料之解壓 (伸長) 處理構成圖。

圖 6 1 係顯示存儲信息之構成例 (例 1) 圖。

圖 6 2 係顯示存儲信息之構成例 1 中的再生處理流程圖。

圖 6 3 係顯示存儲信息之構成例 (例 2) 圖。

圖 6 4 係顯示存儲信息之構成例 2 中的再生處理流程圖。

圖 6 5 係顯示存儲信息之構成例 (例 3) 圖。

圖 6 6 係顯示存儲信息之構成例 3 中的再生處理流程圖。

本說明書所載之圖式係以簡化之圖式表示。

五、發明說明 (254)

圖。

圖 6 7 係顯示存儲信息之構成例 (例 4) 圖。

圖 6 8 係顯示存儲信息之構成例 4 中的再生處理流程圖。

圖 6 9 係用以說明對於存儲資料之生成、容納處理圖。

圖 7 0 係顯示關於存儲資料之容納處理例 (例 1) 的處理流程圖。

圖 7 1 係顯示存儲資料之容納，再生處理中被使用資料管理檔案構成 (例 1) 圖。

圖 7 2 係顯示關於存儲資料之再生處理例 (例 1) 的處理流程圖。

圖 7 3 係顯示關於存儲資料之容納處理例 (例 2) 的處理流程圖。

圖 7 4 係顯示關於存儲資料之再生處理例 (例 2) 的處理流程圖。

圖 7 5 係顯示關於存儲資料之容納處理例 (例 3) 的處理流程圖。

圖 7 6 係顯示存儲資料之容納，再生處理中被使用資料管理檔案構成 (例 2) 圖。

圖 7 7 係顯示關於存儲資料之再生處理例 (例 3) 的處理流程圖。

圖 7 8 係顯示關於存儲資料之容納處理例 (例 4) 的處理流程圖。

本說明書所載之圖式係以簡化之圖式表示。

五、發明說明 (255)

圖 7 9 係顯示關於存儲資料之再生處理例 (例 4) 的處理流程圖。

圖 8 0 係顯示關於存儲資料之容納處理例 (例 5) 的處理流程圖。

圖 8 1 係顯示存儲資料之容納，再生處理中被使用資料管理檔案構成 (例 3) 圖。

圖 8 2 係顯示關於存儲資料之再生處理例 (例 5) 的處理流程圖。

圖 8 3 係顯示關於存儲資料之容納處理例 (例 6) 的處理流程圖。

圖 8 4 係顯示存儲資料之容納，再生處理中被使用資料管理檔案構成 (例 4) 圖。

圖 8 5 係顯示關於存儲資料之再生處理例 (例 6) 的處理流程圖。

圖 8 6 係用以說明存儲信息不正當利用者排除 (Revocation) 構成圖。

圖 8 7 係顯示存儲信息不正當利用者排除 (Revocation) 之處理流程 (例 1) 圖。

圖 8 8 係顯示存儲信息不正當利用者排除 (Revocation) 之處理流程 (例 2) 圖。

圖 8 9 係用以說明安全晶片之構成 (例 1) 圖。

圖 9 0 係顯示安全晶片之製造方法中之處理流程圖。

圖 9 1 係用以說明安全晶片之構成 (例 2) 圖。

圖 9 2 係顯示安全晶片 (例 2) 中之資料寫入處理中

本說明書所載之圖式係以簡化之圖式表示。

AT
BT五、發明說明(256)
的處理流程圖。

圖93係顯示安全晶片(例2)中之寫入處理資料於處理中的處理流程圖。

【元件編號之說明】

- 100...主CPU。
- 107...RAM。
- 108...ROM。
- 109...AV處理部。
- 110...輸入感測部。
- 111...PIO。
- 112...SIO。
- 300...記錄再生部。
- 301...控制部。
- 302...暗號處理部。
- 303...記錄保護控制部。
- 304...讀取部。
- 305...通訊部。
- 306...控制部。
- 307...內部記憶部。
- 308...暗號/密碼化部。
- 400...記錄裝置。
- 401...暗號處理部。
- 402...外部記憶部。

本國際式專利申請案係根據CNS1466規格(207+207公厘) - 259 -

AT
BT

五、發明說明(257)

- 403...控制部。
- 404...通訊部。
- 405...內部記憶部。
- 406...暗號/密碼化部。
- 407...外部記憶部。
- 500...裝置。
- 600...通訊裝置。
- 2101、2102、2103...記錄再生部。
- 2104、2105、2106...記錄裝置。
- 2901...指令號碼管理部。
- 2902...指令寄存器。
- 2903、2904...記錄地址。
- 3001...暗號部。
- 3002...裝置。
- 3090...記憶部。
- 3091...數據信息解析部。
- 3092...資料記憶部。
- 3093...複式記憶部。
- 3094...壓縮伸長處理部。
- 7701...存儲信息資料。
- 7702...刪除(Revocation)。
- 7703...名單控制部。
- 8000...安全晶片。
- 8001...處理部。

本國際式專利申請案係根據CNS1466規格(207+207公厘) - 260 -

AT
BT

五、發明說明(258)

- 8002...記憶部。
- 8003...模式信號線。
- 8004...指令信號線。
- 9201...讀出寫入併用信號。
- 9202...寫入專用信號。

本國際式專利申請案係根據CNS1466規格(207+207公厘) - 261 -

AT
BT

六、申請專利範圍

1. 一種資料處理裝置，係藉由記憶媒體或通訊媒體進行提供之存儲信息資料的處理，其特徵在於具有：
 - 暗號處理部，對前述存儲信息資料用以執行該處理；及
 - 控制部，對前述暗號處理部用以執行控制；
 而前述暗號處理部，其構成係具有：
 - 將存儲信息資料構成部分分割成複數部分後之部分資料對合1以上部分資料集合後為核對值並用以生成部分核對值，並藉由該部分生成後之部分核對值之核對處理用以執行前述部分資料之驗證處理；同時
 - 至少將前述部分核對值核對合1以上部分核對值集合資料列用以生成中間核對值，並使用該生成後之中間核對值，對該部分核對值用以生成前述部分核對值集合之複數的部分核對值對合後之部分資料集合全體用以執行驗證處理。
2. 如申請專利範圍第1項所記載之資料處理裝置，其中前述部分核對值，係將形成核對對象之部分資料作為信息，並藉由用以適用部分核對值生成暗號後之暗號處理生成之值。
- 而前述中間核對值，係將形成核對對象之部分核對值集合資料列作為信息，並藉由適用暗號對值生成暗號後之暗號處理生成之值。
- 而前述暗號處理部，其構成係具有用以對前述部分核對值生成暗號及暗號核對值生成暗號。
3. 如申請專利範圍第2項所記載之資料處理裝置，

本國際式專利申請案係根據CNS1466規格(207+207公厘) - 262 -

六、申請專利範圍

其中前述增號處理部，係具有增號處理之部分核對值生成部以對應於生成之部分核對值。

4. 如申請專利範圍第2項所記載之資料處理裝置，其中前述增號處理係DES增號處理。

而前述增號處理部，係具有可執行DES增號處理之構成。

5. 如申請專利範圍第1項所記載之資料處理裝置，其中前述部分核對值，係將形成核對對象之部分資料鍵值信息在DES-CBC模式中生成或信息經密碼裝（MAC）。

而前述中間核對值，係將形成核對對象之部分核對值與資料鍵值信息在DES-CBC模式中生成或信息經密碼裝（MAC）。

而前述增號處理部，係具有藉由DES-CBC模式用以執行增號處理之構成。

6. 如申請專利範圍第5項所記載之資料處理裝置，其中藉由前述增號處理部具有之DES-CBC模式的增號處理構成，係在形成核對對象之信息列的一部分被適用三倍的DES之構成。

7. 如申請專利範圍第1項所記載之資料處理裝置，其中前述資料處理裝置，係具有署名功能。

而前述增號處理部，係對前述中間核對值藉由適用前記署名功能後之增號處理將生成之值作了資料鍵值信息核對值進行適用之

本願書及說明書中圖式與圖例（CN）A案（210/270/0）

六、申請專利範圍

構成。

8. 如申請專利範圍第7項所記載之資料處理裝置，其中前述資料處理裝置，係做為署名裝置或具有不同種數之署名功能。

而前述增號處理部，係具有根據前述存儲信息資料之利用限制而採用前述不同種數之署名功能將該增號後之署名功能對前述中間核對值進行適用以增號處理為資料鍵值信息核對值之構成。

9. 如申請專利範圍第8項所記載之資料處理裝置，其中前述資料處理裝置，係做為前述種數之署名功能，具有用以執行資料驗證處理及系統之全量體的共同署名功能，及用以執行資料驗證處理之各值的裝置即有之裝置而署名功能。

10. 如申請專利範圍第1項所記載之資料處理裝置，其中前述部分核對值，係含：無部分核對值，對於用以構成資料之一部分的無管部內資料被生成1以上；及存儲信息核對值，對於用以構成資料之一部分的存儲信息區段資料被生成1以上；

而前述增號處理部，其構成係具有對於前述無管部內資料之部分資料集合用以生成1以上之無管部分核對值並用以執行核對處理，而對於前述存儲信息區段資料之部分資料集合用以生成1以上之存儲信息核對值並用以執行核對處理，進而，根據被生成後之前述無管部分核對值及前述

本願書及說明書中圖式與圖例（CN）A案（210/270/0）

六、申請專利範圍

存儲信息核對值全部用以生成核對值並藉由用以執行核對處理用以執行資料驗證。

11. 如申請專利範圍第1項所記載之資料處理裝置，其中前述部分核對值，係含無管部分核對值，對於用以構成資料之一部分的無管部內資料被生成1以上。

而前述增號處理部，其構成係具有對於前述無管部內資料之部分資料集合用以生成1以上之無管部分核對值並用以執行核對處理，進而，用以構成被生成後之前述1以上之無管部分核對值及前述資料之一部分被適用存儲信息區段資料所構成資料用以生成核對值並藉由用以執行核對處理用以執行資料驗證。

12. 如申請專利範圍第1項所記載之資料處理裝置，其中前述資料處理裝置，係具有署名功能。

具有署名功能用以對前述增號處理部中之正當性驗證核對值執行核對處理。

13. 如申請專利範圍第12項所記載之資料處理裝置，係將前述增號處理部中之部分核對值的核對處理中，在核對值未成立時，

而前述核對部，係對前述記錄裝置具有用以中止前記處理之構成。

14. 如申請專利範圍第1項所記載之資料處理裝置，其中前述資料處理裝置，係進而具有再生處理部在前記增號處理部中以再生正當性驗證核對值之資料。

本願書及說明書中圖式與圖例（CN）A案（210/270/0）

六、申請專利範圍

15. 如申請專利範圍第14項所記載之資料處理裝置，其中前述資料處理裝置，係在前述增號處理部中之部分核對值的核對處理中，在核對值未成立時，

而前述核對部，係在前述再生處理部具有用以中止再生處理之構成。

16. 如申請專利範圍第14項所記載之資料處理裝置，其中前述資料處理裝置，係具有控制裝置在前述增號處理部中之部分核對值的核對處理中，僅用以執行資料之無管部分核對值的核對處理，並對成立無管部分核對值之核對後的資料核對到前述再生處理部並做為可再生。

17. 一種資料處理裝置，藉由記憶媒體或通訊媒體提供提供之存儲信息資料的處理，其特徵在於具有：增號處理部，對前述存儲信息資料用以執行增號處理；及

控制部，對前述增號處理部用以執行控制；而前述增號處理部，其構成係具有：

被驗證對象資料有增號化資料時，藉由該增號化資料之譯碼處理部取得譯碼後資料用以執行譯碼處理部取得譯碼處理結果資料藉由用以實施前記署名功能取後之增號處理，用以生成核對值對對象資料之核對值。

18. 如申請專利範圍第17項所記載之資料處理裝置，其中前述增號處理部，係藉由前述增號化資料之譯碼處

本願書及說明書中圖式與圖例（CN）A案（210/270/0）

六、申請專利範圍

將所接收之存儲資訊資料以固定單元位進行餘數驗證與錯誤之處理者。

19. 一種資料處理方法，藉由記憶庫或通訊網路進行數據之存儲信息資料的處理，其特徵在於：

將存儲信息資料分成部分生成數部分之部分資料對合1以上部分資料集合為核對對象並用以生成部分核對值，繼而用以核對生成部分核對值之處理用以執行前述部分資料之驗證處理。

而至少將前述部分核對值與核對值1以上部分核對值集合資料列用以生成中間核對值，並使用該生成中間核對值對應於用以構成前述部分核對值之集合之複數的部分核對值對合之部分資料集合全體用以執行驗證處理。

20. 如申請專利範圍第19項所記載之資料處理方法，其中前述部分核對值，係將前述部分核對值之部分資料作為信息，具有藉由用以適用前述部分核對值生成該之驗證處理生成之值。

而前述中間核對值，係將前述部分核對值之部分核對值集合資料列為信息，具有藉由用以適用該核對值生成驗證處理之值。

21. 如申請專利範圍第20項所記載之資料處理方法，其中前述部分核對值，係對於進行生成之部分核對值使用以適用不重複核對值之部分核對值生成驗證處理者。

22. 如申請專利範圍第20項所記載之資料處理方

本國際式分類法中中國國際分類 (CIP) A46B1 (200705) 號

-267-

六、申請專利範圍

法，其中前述驗證處理係有DES時變處理者。

23. 如申請專利範圍第19項所記載之資料處理方法，其中：

前述部分核對值，係將前述核對對象之部分資料作為信息並在DES-CBC模式中生成或生成信息認證符號 (MAC)，而前述中間核對值，係將前述核對對象之部分核對值集合資料列作為信息並在DES-CBC模式中生成或生成信息認證符號 (MAC)。

24. 如申請專利範圍第19項所記載之資料處理方法，係在所述資料處理方法中，進而：

將前述中間核對值係藉由適用著名驗證之驗證處理將該生成之值為資料驗證值為核對值並加以適用者。

25. 如申請專利範圍第24項所記載之資料處理方法，係在所述資料處理方法中，進而：

根據資料之利用而影響選擇不同著名驗證對前述中間核對值適用時驗證處理為資料驗證值為核對值。

26. 如申請專利範圍第25項所記載之資料處理方法，係在所述資料處理方法中：

做為前述著名驗證，係利用以執行資料驗證處理共同於系統之全實體之共同著名驗證，及用以執行資料驗證處理之各個實體間有的實體具有著名驗證根據資料之利用限制選擇進行選擇並加以使用。

27. 如申請專利範圍第19項所記載之資料處理方法，係在所述資料處理方法中：

本國際式分類法中中國國際分類 (CIP) A46B1 (200705) 號

-268-

六、申請專利範圍

前述部分核對值，係合：集部分核對值，對於用以構成資料之一部分之集管部內資料被生成1以上，及存儲信息核對值，對於用以構成資料之一部分之存儲信息部內資料被生成1以上；

而前述資料驗證處理，係對於前述集管部內資料之部分資料集合用以生成1以上之集管部分核對值並用以執行核對處理。

而對於前述存儲信息部內資料之部分資料集合用以生成1以上之存儲信息核對值並用以執行核對處理。

進而，根據被生成之前述集管部分核對值及前述存儲信息核對值全部用以生成核對值並用以執行資料驗證處理。

28. 如申請專利範圍第19項所記載之資料處理方法，係在所述資料處理方法中：

前述部分核對值，係合集管部分核對值，對於用以構成資料之一部分之集管部內資料被生成1以上。

而前述資料驗證處理，係對於前述集管部內資料之部分資料集合用以生成1以上之集管部分核對值並用以執行核對處理。

進而，用以構成被生成之前述1以上之集管部分核對值及前述資料之一部分根據由存儲信息部資料所用資料列用以生成核對值並藉由用以執行核對處理用以執行資料驗證處理。

29. 如申請專利範圍第19項所記載之資料處理方

本國際式分類法中中國國際分類 (CIP) A46B1 (200705) 號

-269-

六、申請專利範圍

法，係在所述資料處理方法中：

資料之驗證處理，進而，將驗證處理資料合密於記錄裝置之處理。

30. 如申請專利範圍第29項所記載之資料處理方法，係在所述資料處理方法中：

前述部分核對值之核對處理中，使核對未成立之情形中，用以中止前述處理而前述記錄裝置並用以執行控制。

31. 如申請專利範圍第19項所記載之資料處理方法，係在所述資料處理方法中：

資料之驗證處理，合用以再生資料之資料再生處理者。

32. 如申請專利範圍第31項所記載之資料處理方法，係在所述資料處理方法中：

前述部分核對值之核對處理中，使核對未成立之情形中，在所述再生處理部用以中止再生處理並用以執行控制。

33. 如申請專利範圍第31項所記載之資料處理方法，係在所述資料處理方法中：

在所述部分核對值之核對處理中，通用以執行資料之集管部分核對值的核對處理，將成立集管部分核對值之核對的資料轉送到前述再生處理部而再生並用以執行控制者。

34. 一種資料處理方法，係藉由記憶庫或通訊網路進行被提供之存儲信息資料之處理，其特徵在於：

驗證並對資料有暗號化資料時，藉由該暗號化資料

本國際式分類法中中國國際分類 (CIP) A46B1 (200705) 號

-270-

六、申請專利範圍

而前述增設處理部，係根據收容於前述記憶部後之駁誌輸出生成用主輸出 Make，及前述外部連接裝置之識別資料的外部連接裝置識別子用以執行增設處理，並用以生成前述外部連接裝置之駁誌輸出 Make 的構成。

5 0. 如申請專利範圍第 4 7 項所記載之資料處理裝置，其中前述資料處理裝置，係對資料利用執行署名處理的資料處理裝置。

而前述記憶部，係具有用以生成前述資料處理裝置之資料處理裝置署名名義 Kdev 並用以收容署名名義生成用主輸出 MKdev。

而前述增設處理部，係根據收容於前述記憶部之署名名義生成用主輸出 MKdev，及前述資料處理裝置之識別資料的資料處理裝置識別子用以執行增設處理，並用以生成前述資料處理裝置之資料處理裝置署名名義 Kdev 的構成。

5 1. 如申請專利範圍第 4 7 項所記載之資料處理裝置，係對用以執行增設處理必要之個別輸出，根據前述主輸出，及增設處理對象之裝置或資料之識別資料進行生成之個別輸出生成處理。

係將增設處理對象之裝置或資料之識別資料至少一部分作為信息，並將前述主輸出與增設輸出進行適用之增設處理。

5 2. 如申請專利範圍第 5 1 項所記載之資料處理裝置，其中前述增設處理係適用 D B S 算法之增設處理。

本局式及適用申請專利範圍第 4 7 項 (C4) A4 號 (310X297 分卷)

- 275 -

六、申請專利範圍

5 3. 一種資料處理系統，係由複數之資料處理裝置構建之資料處理系統中，其特徵在於：

提供複數個之資料處理裝置的各自，具有共同之主輸出為用以生成適用於資料增設化，資料譯碼化，資料驗證，認證處理，署名處理至少其中之一之增設處理之輸出。

並使前述複數之資料處理裝置的各自，具有前述主輸出，及增設處理對象之裝置或資料之識別資料用以生成執行前述增設處理必要之共同之個別輸出的構成。

5 4. 如申請專利範圍第 5 3 項所記載之資料處理系統，其中前述複數之資料處理裝置，

係藉由提供存儲信息資料之存儲信息資料提供裝置，及進行利用存儲信息資料之存儲信息資料利用裝置構建。

並使存儲信息資料提供裝置及存儲信息資料利用裝置之雙方，具有前述輸出生成用主輸出適用於前述存儲信息資料提供裝置及存儲信息資料利用裝置間之流通存儲信息資料的增設處理為用以生成存儲信息資料配送輸出。

而前述存儲信息資料提供裝置，係具有前述前述配送輸出生成用主輸出，及提供存儲信息資料之識別子之存儲信息資料識別子用以生成存儲信息資料配送輸出，並用以執行該存儲信息資料之增設化處理。

並透過存儲信息資料利用裝置，係根據前述配送輸出生成用主輸出，及存儲信息資料之識別子之存儲信息資料

本局式及適用申請專利範圍第 5 3 項 (C4) A4 號 (310X297 分卷)

- 276 -

六、申請專利範圍

子用以生成存儲信息資料配送輸出，並用以執行該存儲信息資料之譯碼化處理的構成。

5 5. 如申請專利範圍第 5 4 項所記載之資料處理系統，其中前述存儲信息資料提供裝置，係具有複數不同之配送輸出生成用主輸出為用以生成複數不同之存儲信息資料配送輸出，並根據該複數之配送輸出生成用主輸出及前述存儲信息資料識別子用以生成複數不同之存儲信息資料配送輸出，藉由該生成之複數的配送輸出用以執行增設化處理並用以生成複數個之增設化存儲信息資料。

而前述存儲信息資料利用裝置，係具有前述存儲信息資料提供裝置的複數不同之配送輸出生成用主輸出至少 1 個之配送輸出生成用主輸出，使用自己所有之配送輸出生成用主輸出及同樣配送輸出生成用主輸出藉由該生成之配送輸出進行增設化存儲信息資料可譯碼之構成。

5 6. 如申請專利範圍第 5 3 項所記載之資料處理系統，係在前述複數之資料處理裝置的各自，用以寄附同一之存儲信息輸出生成用主輸出為用以生成適用於存儲信息資料之增設處理的存儲信息輸出。

並在前述複數之資料處理裝置之一個資料處理裝置 A 中，根據前述存儲信息輸出生成用主輸出，及該資料處理裝置 A 之裝置識別子藉由該生成之存儲信息輸出被增設化並被收容於記憶部後之存儲信息資料。

在不同資料處理裝置 B 中，根據前述同一之存儲信息輸出生成用主輸出，及前述資料處理裝置 A 之裝置識別子

本局式及適用申請專利範圍第 5 3 項 (C4) A4 號 (310X297 分卷)

- 277 -

六、申請專利範圍

用以生成存儲信息輸出，並根據該生成之存儲信息輸出，在前述資料處理裝置 A 中用以執行寄附於前述記憶部後之增設化存儲信息資料之譯碼處理的構成。

5 7. 如申請專利範圍第 5 3 項所記載之資料處理系統，其中前述複數之資料處理裝置，

係藉由主裝置，及形成該主裝置之認證對象的副裝置構建。

並透過主裝置及副裝置之雙方，具有前述輸出生成用主輸出適用於主裝置及副裝置間之認證處理。

而前述副裝置，係具有前述前述配送輸出生成用主輸出，及該副裝置之識別子之副裝置識別子用以生成配送輸出並寄附於副裝置內記憶。

而前述主裝置，係根據前述配送輸出生成用主輸出，及該副裝置之識別子之副裝置識別子用以生成配送輸出並用以執行認證處理之構成。

5 8. 一種資料處理方法，用以執行資料增設化，資料譯碼化，資料驗證，認證處理，署名處理至少其中之一之增設處理的資料處理方法中，其特徵在於具有：

將用以執行增設處理必要之個別輸出，根據為用以生成適用於前述增設處理之輸出的主輸出，及根據該識別子之裝置或資料之識別資料生成之配送輸出步驟；及

藉由前述配送輸出多步驟根據進行生成之配送輸出用以執行增設處理之增設處理步驟。

5 9. 如申請專利範圍第 5 8 項所記載之資料處理方

本局式及適用申請專利範圍第 5 3 項 (C4) A4 號 (310X297 分卷)

- 278 -

六、申請專利範圍

法，在前述資料處理方法中進行執行的資料處理，係透過記錄媒體或通訊媒體將轉送資料之時號處理。

而前述轉送生成步驟，

係根據用以生成適用於轉送資料之時號處理的配送輪點 Kdis 之配送輪點生成用主輪點 Mdis，及前述轉送資料之識別資料的資料識別子用以執行時號處理，並用以生成前述轉送資料之配送輪點 Kdis 之配送輪點生成步驟，

而前述時號處理步驟，

係根據前述配送輪點生成步驟中之生成的配送輪點 Kdis 用以執行轉送資料之時號處理的步驟。

00、如申請專利範圍第 58 項所記載之資料處理方法，其中前述資料處理方法中之進行執行的資料處理，係形成轉送資料之轉送對象或轉送對象的外部處理裝置之認證處理，

而前述轉送生成步驟，係根據用以生成前述外部處理裝置之認證輪點 Kake 的認證輪點生成用主輪點 Mlake，及前述外部處理裝置之識別資料的外部處理裝置識別子用以執行時號處理，並用以生成前述外部處理裝置之認證輪點 Kake 的認證輪點生成步驟，

而前述時號處理步驟，係根據前述認證輪點生成步驟中進行生成之認證輪點 Kake 用以執行外部處理裝置之認證處理的步驟。

01、如申請專利範圍第 58 項所記載之資料處理方法，其中前述資料處理方法中之進行執行的資料處理，係

本申請案之技術方案係根據 (CNS) A48 號 (2006/2710 號)。

六、申請專利範圍

對資料之署名處理，

而前述輪點生成步驟，

係根據用以生成前述資料處理裝置之資料處理裝置署名輪點 Kdev 的署名輪點生成用主輪點 Mdev，及前述資料處理裝置之識別資料的資料處理裝置識別子用以執行時號處理，並用以生成前述資料處理裝置之資料處理裝置署名輪點 Kdev 的署名輪點生成步驟，

而前述時號處理步驟，

係根據前述署名輪點生成步驟中之進行生成之署名輪點 Kdev 用以執行資料之署名處理的步驟。

02、如申請專利範圍第 58 項所記載之資料處理方法，其中前述輪點生成步驟，

係將時號處理對象之能量或資料之識別資料至少一部分放為信息，並將前述主輪點做為時號輪點進行適用之時號處理。

03、如申請專利範圍第 62 項所記載之資料處理方法，其中前述時號處理係適用 DES 算法之時號處理。

04、一種資料處理方法，由提供存儲信息資料之存儲信息資料提供裝置，及進行存儲信息資料之利用的存儲信息資料利用裝置所構成資料處理系統中之資料處理方法，其特徵在於：

前述存儲信息資料提供裝置，係根據為了用以生成適用於存儲信息資料之時號處理的存儲信息資料配送輪點之配送輪點生成用主輪點，及提供存儲信息資料之識別子約

本申請案之技術方案係根據 (CNS) A48 號 (2006/2710 號)。

六、申請專利範圍

存儲信息識別子用以生成存儲信息資料配送輪點，並用以執行該存儲信息資料之時號化處理，

而前述存儲信息資料利用裝置，係根據前述配送輪點生成用主輪點，及提供存儲信息資料之識別子約的存儲信息識別子用以生成存儲信息資料配送輪點，並用以執行該存儲信息資料之時號化處理。

05、如申請專利範圍第 54 項所記載之資料處理方法，其中前述存儲信息資料提供裝置，係具有複數不同之配送輪點生成用主輪點為用以生成複數不同之存儲信息資料配送輪點，並根據該複數之配送輪點生成用主輪點及前述存儲信息識別子用以生成複數不同之存儲信息資料配送輪點，藉由該生成之複數的配送輪點用以執行時號化處理並用以生成複數不同之時號化存儲信息資料。

而前述存儲信息資料利用裝置，係具有前述存儲信息資料提供裝置有的複數不同之配送輪點生成用主輪點至少 1 個之配送輪點生成用主輪點，使用自己所有之配送輪點生成用主輪點及同樣配送輪點生成用主輪點經由該生成之配送輪點而將時號化存儲信息資料進行處理。

06、一種資料處理方法，係由複數之資料處理裝置構成資料處理系統中之資料處理方法，其特徵在於具有：

在前述複數之資料處理裝置中之 1 個資料處理裝置 A 中，係儲存存儲信息資料生成用主輪點為了用以生成適用於存儲信息資料之時號處理的存儲信息識別子，及該資料處理

本申請案之技術方案係根據 (CNS) A48 號 (2006/2710 號)。

六、申請專利範圍

裝置 A 之裝置識別子藉由該生成之存儲信息輪點而將時號化之存儲信息資料存納於記憶媒體之步驟。

在不同資料處理裝置 B 中，係根據前述資料處理裝置 A 及同一之前述存儲信息輪點生成用主輪點及前述資料處理裝置 A 之裝置識別子用以生成前述存儲信息輪點及同一存儲信息輪點之步驟，及

在前述資料處理裝置 B 藉由該生成之存儲信息輪點進行存納於前述記憶媒體之存儲信息資料之讀取的步驟。

07、一種資料處理方法，由主裝置，及形成該主裝置之認證處理對象的副裝置所構成之資料處理系統中之資料處理方法，

前述副裝置，係根據該認證輪點生成用主輪點為了用以生成適用於主裝置及副裝置間之認證處理的認證輪點，及該副裝置之識別子約的副裝置識別子用以生成認證輪點，並由該生成之認證輪點存納於該副裝置內之記憶體。

而前述主裝置，係根據前述認證輪點生成用主輪點，及前述副裝置之識別子約的副裝置識別子用以生成認證輪點並用以執行認證處理。

08、一種程式提供媒體，係用以提供電腦程式並用以執行資料時號化、資料譯碼化、資料驗證、認證處理、署名處理至少其中之一之時號處理並將時號處理在電腦系統上執行之程式提供媒體，其特徵在於：

該執行時號處理必要之識別輪點，根據主輪點為了用

本申請案之技術方案係根據 (CNS) A48 號 (2006/2710 號)。

六、申請專利範圍

以生成須用於前述驗證處理之輸出，及隨後處理對之驗證資料之識別資料進行生成之輸出之處理步驟；及

藉由前述輸出之處理步驟生成後之輸出以執行驗證處理之驗證處理步驟。

69. 一種資料處理裝置，係藉由記憶體或通訊媒體進行提供存儲信息資料之處理的資料處理裝置，其特徵在於具有：

記憶部，用以收納資料處理裝置識別子；

名稱驗證部，用以抽出包含於存儲信息資料中之不正當名稱名單，並用以執行該名單內之項目及該名單於前述記憶部之前述資料處理裝置識別子之核對處理；及

控制部，前述核對處理部中之核對處理結果，與含有在前述不正當名稱名單中與前述資料處理裝置識別子進行一致的資訊時，用以中止於前述存儲信息資料之再生或記錄裝置之存儲處理至少其中之一之處理執行。

70. 如申請專利範圍第69項所記載之資料處理裝置，其中前述名稱驗證部，係具有根據處理部用以執行對前述存儲信息資料的驗證處理。

係根據包含於前述存儲信息資料不正當名稱名單之核對部用以驗證有無前述不正當名稱名單的資訊，並藉由該驗證部，係判定形成資訊時用以執行前述核對處理之構成。

71. 如申請專利範圍第70項所記載之資料處理裝置，其中前述資料處理裝置，係具有不正當名稱名單核對

本申請人提出之申請專利範圍 (CNS) A46條 (210×270 mm)

六、申請專利範圍

生成輸出部。

而前述驗證處理部。

係對驗證對象之不正當名稱名單或資料用以執行選用驗證不正當名稱名單核對生成輸出之驗證處理並用以生成不正當名稱名單核對值，並用以執行該驗證生成後之不正當名稱名單核對值，及該核對值於存儲信息資料中不正當名稱名單之核對值的核對並用以驗證有無前述不正當名稱名單之資訊的構成。

72. 如申請專利範圍第69項所記載之資料處理裝置，其中前述名稱驗證部，係具有根據處理部用以執行對前述存儲信息資料之驗證處理。

而前述驗證處理部，係用以執行包含於前述存儲信息資料中被驗證後之不正當名稱名單的譯碼處理，並做為該驗證處理之結果對於核對取得後之不正當名稱名單用以執行前述核對處理之構成。

73. 如申請專利範圍第69項所記載之資料處理裝置，其中前述名稱驗證部，係具有根據處理部用以執行對前述存儲信息資料之轉送對象或轉送部之記錄裝置的相互認證處理。

而前述名稱驗證部，係藉由前述驗證部根據被執行前述記錄裝置之相互認證處理成立認證後而為條件，用以抽出包含於前述存儲信息資料中不正當名稱名單或資料於前述記憶部之前述資料處理裝置識別子用以執行核對處理之構成。

本申請人提出之申請專利範圍 (CNS) A46條 (210×270 mm)

六、申請專利範圍

74. 一種資料處理方法，係藉由記憶體或通訊媒體進行提供存儲信息資料之處理的資料處理方法，其特徵係具有：

用以抽出包含於存儲信息資料中不正當名稱名單之名稱輸出步驟；

藉由前述名單抽出步驟被包含於抽出後之名單的項目，及經專利用於資料處理裝置內之記憶部後之前述資料處理裝置識別子用以執行核對處理之核對處理步驟；及

前述核對處理步驟中之核對處理結果，在驗證不正當名稱名單中會有與前述資料處理裝置識別子一致的資訊時，用以中止於前述存儲信息資料之再生或記錄裝置之存儲處理至少其中之一之處理執行之步驟。

75. 如申請專利範圍第74項所記載之資料處理方法，其中前述資料處理方法，係透過：

含根據包含於前述存儲信息資料中不正當名稱名單之核對部用以驗證有無前述不正當名稱名單之資訊的驗證處理步驟。

而前述核對處理步驟。

係藉由前述驗證步驟，進行判定形成資訊時執行執行。

76. 如申請專利範圍第75項所記載之資料處理方法，其中前述驗證步驟。

係對於驗證對象之不正當名稱名單或資料用以執行選用不正當名稱名單核對生成輸出後之驗證處理並用以

本申請人提出之申請專利範圍 (CNS) A46條 (210×270 mm)

六、申請專利範圍

生成不正當名稱名單核對值的步驟，及

用以執行生成後之不正當名稱名單核對值，及該核對值於存儲信息資料中不正當名稱名單核對值的核對並用以驗證有無前述不正當名稱名單之資訊的步驟。

77. 如申請專利範圍第74項所記載之資料處理方法，其中前述資料處理方法，係透過：

含用以執行包含於前述存儲信息資料中被驗證後之不正當名稱名單的譯碼處理之譯碼步驟。

而前述核對處理步驟。

係做為前述譯碼步驟之結果對於核對取得之不正當名稱名單用以執行前述核對處理。

78. 如申請專利範圍第74項所記載之資料處理方法，其中前述資料處理方法，係透過：

含形成存儲信息資料之轉送對象或轉送部與記錄裝置相互認證處理步驟。

而前述核對處理部，係藉由前述相互認證處理步驟執行前述記錄裝置與相互認證處理成立認證後做為條件用以執行前述核對處理。

79. 一種存儲信息資料生成方法，藉由記憶體或通訊媒體對數據之記錄再生部進行提供存儲信息資料之生成的存儲信息資料生成方法，其特徵在於：

做為存儲信息資料之無實質資訊形成存儲信息資料之利用排除對數據記錄再生部之記錄再生部識別子用以導出做為存儲信息資料後之不正當名稱名單並做為存儲信息資料。

本申請人提出之申請專利範圍 (CNS) A46條 (210×270 mm)

六、申請專利範圍

8 0. 如申請專利範圍第 7 項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進而，

係將存儲信息資料之真實資訊，用以容納前述不正常裝置名單之資訊以利用之不正常裝置名單相對結果。

8 1. 如申請專利範圍第 7 項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進而，將前述不正常裝置名單進行唯號化並用以容納於存儲信息資料之真實資訊中者。

8 2. 一程式提供設備，用以提供電腦程式經由記憶媒體或通訊媒體提供存儲信息資料之處理在電腦系統上執行的程式提供設備，其特徵在於：前述電腦程式，係具有：

用以抽出包含於存儲信息資料中不正常裝置名單之名單抽出步驟；

藉由前述名單抽出步驟基於抽出之名單的項目，及容納於資訊處理裝置內之記憶後的前述資料處理裝置資訊予以執行相對處理之相對處理步驟；及

前述相對處理步驟中之相對處理結果，在前述不正常裝置名單中含有與前述資料處理裝置進行一致的資訊時，用以中止前述存儲信息資料之生成或對記錄裝置之容納處理至少其中之一之處理執行之步驟。

8 3. 一資料處理裝置，藉由記憶媒體或通訊媒體進行提供存儲信息資料之處理之資料處理裝置，其特徵在於具有：

本報日文版及中文版與本報 (CNS) A1 版 (2009 年 7 月 20 日)

六、申請專利範圍

唯號處理部，對前述存儲信息資料用以執行唯號處理；

控制部，對前述唯號處理部用以執行控制；

系統共同點，被使用於前述唯號處理部中之唯號處理，並共同於利用前述存儲信息資料之其他的資料處理裝置；及

裝置固有識別子至少其中之一，為用以生成被使用於前述唯號處理部中之唯號處理的資料處理裝置固有之裝置固有唯號或裝置固有唯號；

而前述唯號處理部，

係根據前述存儲信息資料之利用態樣將前述系統共同點，或前述裝置固有唯號之其中之一適用於前述存儲信息資料並用以執行唯號處理。

8 4. 如申請專利範圍第 8 3 項所記載之資料處理裝置，其中前述唯號處理部，

係其構成具有與前述包含於前述存儲信息資料之利用限制資訊並將前述系統共同點，或前述裝置固有唯號其中之一適用於前述存儲信息資料並用以執行唯號處理。

8 5. 如申請專利範圍第 8 3 項所記載之資料處理裝置，其中前述資料處理裝置，係進而，

具有記錄裝置用以記錄存儲信息資料。

而前述唯號處理部，

係將前述存儲信息資料存放在自己之資料處理裝置並附有使用之利用限制時，對前述存儲信息資料使用前述裝置固有唯號。

本報日文版及中文版與本報 (CNS) A1 版 (2009 年 7 月 20 日)

六、申請專利範圍

裝置固有唯號用以執行唯號處理並用以生成容納資料到前述記錄裝置之。

並將前述存儲信息資料放在自己之資料處理裝置以外之裝置也可被為使用時，對前述存儲信息資料使用前述系統共同點並用以執行唯號處理並用以生成容納資料到前述記錄裝置之構成。

8 6. 如申請專利範圍第 8 3 項所記載之資料處理裝置，其中前述資料處理裝置，

係具有資料處理裝置固有之署名名稱 Kdev，及在裝置之資料處理裝置共同之系統署名名稱 Ksys，

而前述唯號處理部，

係將前述存儲信息資料存放在自己之資料處理裝置附有使用之利用限制時並容納於前述記錄裝置時，對前述存儲信息資料適用前述裝置固有之署名名稱 Kdev 藉由唯號處理用以生成裝置固有唯號對值。

並將前述存儲信息資料存放在自己之資料處理裝置以外之裝置也可被為使用且容納於前述記錄裝置時，對前述存儲信息資料適用前述系統署名名稱 Ksys 後藉由唯號處理用以生成系統對值。

而前述控制部，

係將前述唯號處理部之生成後的前述裝置固有唯號對值或前述系統對值之一與前述存儲信息資料一起容納於前述記錄裝置用以執行控制。

8 7. 如申請專利範圍第 8 3 項所記載之資料處理裝

本報日文版及中文版與本報 (CNS) A1 版 (2009 年 7 月 20 日)

六、申請專利範圍

置，其中前述資料處理裝置，

係具有資料處理裝置固有之署名名稱 Kdev，及在裝置之資料處理裝置共同之系統署名名稱 Ksys，

而前述唯號處理部，

係係放在自己之資料處理裝置用以可生被附有使用之利用限制的存儲信息資料時，對前述存儲信息資料適用前述裝置固有之署名名稱 Kdev 後藉由唯號處理用以生成裝置固有唯號對值，並用以執行該生成後之唯號對值核對值的核對處理。

而放在自己之資料處理裝置以外的裝置也被被為可應用用以可生被附有利用限制的存儲信息資料時，對前述存儲信息資料適用前述系統署名名稱 Ksys 後藉由唯號處理用以生成系統對值，並用以執行該生成後之系統對值的核對處理。

而前述控制部，

係係將前述裝置固有唯號對值之核對成立後時，或係使前述系統對值之核對成立後時以存儲信息資料之唯號處理部被處理後用以生成可再生產資料之構成。

8 8. 如申請專利範圍第 8 3 項所記載之資料處理裝置，其中前述資料處理裝置，

係具有記錄資料處理裝置署名名稱 IDdev，及資料處理裝置識別子 IDdev，

而前述唯號處理部，

係根據前述資料處理裝置署名名稱 IDdev 及

本報日文版及中文版與本報 (CNS) A1 版 (2009 年 7 月 20 日)

六、申請專利範圍

前述資料處理裝置係屬於 IDdev 藉由硬體處理後為資料處理裝置固有輪胎用以生成署名輪胎 Kdev。

8 9. 如申請專利範圍第 8 項所記載之資料處理裝置，其中前述硬體處理部，

係對前述資料處理裝置屬於 IDdev 適用前述資料處理裝置署名輪胎用以生成署名輪胎 D E S 時該處理用以生成前述署名輪胎之構成。

9 0. 如申請專利範圍第 8 項所記載之資料處理裝置，其中前述硬體處理部，

係對前述存儲信息資料用以執行時該處理用以生成中間核對值，在該中間核對值適用前述資料處理裝置固有輪胎或系統共有輪胎用以執行時該處理。

9 1. 如申請專利範圍第 9 0 項所記載之資料處理裝置，其中前述硬體處理部，

係將前述存儲信息資料分割成該數部分後之部分資料對合 1 以上之部分資料集合藉由前述處理用以生成部分核對值。

而合生成後之部分核對值對該部分核對值集合資料列藉由硬體處理用以生成中間核對值之構成。

9 2. 一種資料處理方法，藉由該硬體或該軟體進行提供存儲信息資料之處理的資料處理方法，其特徵在於：

根據該存儲信息資料之利用關係，

用以選擇利用前述存儲信息資料共處於其他資料處理

本國際大英商標局註冊第 (CNS) A 類第 (2109/270) 號。

六、申請專利範圍

裝置之時該處理用系統共同處理，或，資料處理裝置固有之裝置固有輪胎其中之一之時該處理輪胎。

將處理後之輪胎處理後並適用於前述存儲信息資料用以執行時該處理。

9 3. 如申請專利範圍第 9 2 項所記載之資料處理方法，其中前述資料處理方法中，

用以選擇該處理輪胎之步驟，係根據該合於前述存儲信息資料之利用限制資訊進行選擇之步驟。

9 4. 如申請專利範圍第 9 2 項所記載之資料處理方法，係對前述資料處理方法中之存儲信息資料的記錄裝置之記錄處理中，

將該存儲信息資料置於自己之資料處理裝置內所製，對該存儲信息資料使用前述裝置固有輪胎用以執行時該處理並用以生成存儲資料對前述記錄裝置。

而將前述存儲信息資料也置於自己之資料處理裝置以外之裝置也使用時，對該存儲信息資料使用前述系統共同輪胎使用用以執行時該處理並用以生成存儲資料對前述記錄裝置。

9 5. 如申請專利範圍第 9 2 項所記載之資料處理方法，對前述資料處理方法中之存儲信息資料的記錄裝置之記錄處理中，

將前述存儲信息資料僅置於自己之資料處理裝置內有使用之利用限制並容納於前述記錄裝置時，對前述存儲信息資料適用前述裝置固有之署名輪胎 Kdev 後藉由時該處理

本國際大英商標局註冊第 (CNS) A 類第 (2109/270) 號。

六、申請專利範圍

用以生成裝置固有核對值。

將前述存儲信息資料置於自己之資料處理裝置以外的裝置也使用時容納於前述記錄裝置時，對前述存儲信息資料適用前述系統署名輪胎 Ksys 後藉由時該處理用以生成核對值。

並將前述生成後之核對值裝置固有核對值與前述核對值其中之一與前述存儲信息資料一起容納於前述記錄裝置。

9 6. 如申請專利範圍第 9 2 項所記載之資料處理方法，係前該資料處理方法中之存儲信息資料的產生處理中，

僅置於自己之資料處理裝置用以再生後有使用之利用限制後的存儲信息資料時，對前述存儲信息資料適用前述裝置固有之署名輪胎 Kdev 後藉由時該處理用以生成裝置固有核對值，並用以執行該生成後之裝置固有核對值的核對處理。

而置於自己之資料處理裝置以外之裝置使用時容納於前述記錄裝置時，對前述存儲信息資料適用前述系統署名輪胎 Ksys 後藉由時該處理用以生成核對值，並用以執行該生成後之核對值的核對處理。

成立前述裝置固有核對值之核對值時，或係成立該核對值時之核對值時用以執行時該存儲信息資料之再生。

9 7. 如申請專利範圍第 9 2 項所記載之資料處理方法

本國際大英商標局註冊第 (CNS) A 類第 (2109/270) 號。

六、申請專利範圍

法，含根據資料處理裝置署名輪胎用以主輪胎 MKdev 及資料處理裝置屬於 IDdev 藉由硬體處理後為資料處理裝置署名輪胎用以生成署名輪胎 Kdev 之步驟。

9 8. 如申請專利範圍第 9 7 項所記載之資料處理方法，其中前述署名輪胎 Kdev 生成步驟，

係對前述資料處理裝置屬於 IDdev 適用前述資料處理裝置署名輪胎用以主輪胎 MKdev 後藉由 D E S 時該處理用以生成前述署名輪胎 Kdev 之步驟。

9 9. 如申請專利範圍第 9 2 項所記載之資料處理方法，其中前述資料處理方法，係進而，

含對前述存儲信息資料用以執行時該處理並用以生成中間核對值之步驟。

在該適中間核對值適用前述資料處理裝置固有輪胎或系統共有輪胎使用用以執行時該處理。

1 0 0. 如申請專利範圍第 9 9 項所記載之資料處理方法，其中前述資料處理方法，係進而，

將該存儲信息資料分割成該數部分後之部分資料對合 1 以上部分資料集合藉由時該處理用以生成部分核對值。

並對該合生成後之部分核對值之部分核對值集合資料列藉由時該處理用以生成中間核對值。

1 0 1. 一種程式提供軟體，提供電腦程式碼由記憶媒體或通訊媒體進行提供該存儲信息資料之處理資料處理在電腦系統上執行之程式媒體，其特徵在於：

本國際大英商標局註冊第 (CNS) A 類第 (2109/270) 號。

六、申請專利範圍

前述電腦程式：

係根據前述存儲信息資料之利用態樣，

用以選擇利用前述存儲信息資料共同於其他資料處理裝置之唯號處理用系統共同輸出，或，資料處理裝置固有之裝置固有輸出其中之一的唯號處理輸出的步驟。

將溢譯後之暗號處理輸出適用於前述存儲信息資料用以執行暗號處理之步驟。

102. 一種資料處理裝置，藉由記錄媒體或通訊媒體進行被提供存儲信息資料之處理的資料處理裝置，其特徵在於具有：

暗號處理部，對前述存儲信息資料用以執行暗號處理

控制部，對前述暗號處理部用以執行控制；

而前進環境處理部。

係在會於資料驗證對象之存儲信息區段資料單位用以生成存儲信息類對值，藉由用以執行生成後之存儲信息類對值之核對處理，用以執行前述資料中之存儲信息區段資料單位之正確性驗證處理之構成。

103. 如申請專利範圍第102項所記載之資料處理裝置，其中前述資料處理裝置，係具有存儲信息核對值生成輪匙：

而前述兩變處理範

係根據驗證對象之存儲信息區段資料用以生成存儲信息中間值，並對該存儲信息中間值適用前述存儲信息核對

六、申請專利範圍

體通行被提供存儲信息資料之處置的資料處理方法，

係在含於資料驗證對象之存儲信息區段資料單位用以生成存儲信息核對值，藉由用以執行生成後之存儲信息核對值之核對處理，用以執行前述資料中之存儲信息區段資料單位的正確性驗證處理。

116. 如申請專利範圍第115項所記載之資料處理方法，其中前述資料處理裝置，

係根據驗證對象之存儲信息區段資料用以生成存儲信息中間值。

並對生成後之存儲信息中間值適用存儲信息核對值生成驗證後用以執行驗證處理並用以生成存儲信息核對值。

117. 如申請專利範圍第115項所記載之資料處理方法，其中前述資料處理方法，

係使驗證對象之存儲信息區段資料邏輯化時，藉由該存儲信息區段資料之譯碼處理所取得譯碼文全體以預定單元位進行預定之演算處理並用以生成存儲信息中間值。

並使驗證對象之存儲信息區段資料邏輯化時，將存儲信息區段資料全體以預定單元位進行預定之演算處理並用以生成存儲信息中間值。

118. 如申請專利範圍第117項所記載之資料處理方法，其中前述資料處理方法，

在驗證中間值核對值之生成處理進行適用前述預定之演算處理係併性邏輯和演算。

本公開文件係以中文書寫（CNS）A4規格（210×297mm）

六、申請專利範圍

119. 如申請專利範圍第117項所記載之資料處理方法，其中前述存儲信息中間值之生成處理中，

使驗證對象之存儲信息區段資料邏輯化時適用於存儲信息中間值生成處理之前述演算處理，係藉由CBC模式之譯碼處理。

120. 如申請專利範圍第119項所記載之資料處理方法，其中藉由前述CBC模式之譯碼處理構成，係在生成驗證對象之信息列的一部分適用演算式共同驗證處理。

121. 如申請專利範圍第115項所記載之資料處理方法，其中前述資料處理方法中，

在存儲信息區段資料含有複數之零件，並被包含於該存儲信息區段資料一部分之零件驗證對象時，根據驗證對象零件用以生成存儲信息核對值。

並藉由用以執行生成後之存儲信息核對值的核對處理，用以執行前述資料中之存儲信息區段資料單位的正確性驗證處理。

122. 如申請專利範圍第121項所記載之資料處理方法，其中前述資料處理方法中，

在驗證存儲信息區段資料含有複數之零件，使驗證對象之驗證零件有1個時，

使前述驗證零件被核對時，藉由要驗證零件之譯碼處理取得譯碼文全體以預定單元位進行進行驗證處理和核對值，適用存儲信息核對值生成驗證後用以執行驗證處理。

本公開文件係以中文書寫（CNS）A4規格（210×297mm）

六、申請專利範圍

號處理並用以生成存儲信息核對值。

從前述要驗證零件被核對時，將該要驗證零件全體以預定單元位進行排他邏輯和演算之演算，適用前述存儲信息核對值生成驗證後用以執行驗證處理並用以生成存儲信息核對值。

123. 如申請專利範圍第121項所記載之資料處理方法，其中前述資料處理方法中，

在前述存儲信息區段資料含有複數之零件，使驗證對象之驗證零件有複數時，

在各零件適用存儲信息核對值生成驗證後用以執行驗證處理並取得後之零件核對值之邏輯和演算，進而適用前述存儲信息核對值生成驗證後用以執行驗證處理並取得結果後存儲信息核對值。

124. 如申請專利範圍第115項所記載之資料處理方法，其中前述資料處理方法，係並行。

含執行正當性驗證後之存儲信息區段資料合用以生成存儲信息資料的步驟。

125. 如申請專利範圍第124項所記載之資料處理方法，其中前述資料處理方法，係並行。

在存儲信息核對值之核對處理中，在生成驗證對象之情形。

前述控制部，係用以中止驗證處理到驗證記錄裝置。

126. 如申請專利範圍第115項所記載之資料處理方法，其中前述資料處理方法，係並行。

本公開文件係以中文書寫（CNS）A4規格（210×297mm）

六、申請專利範圍

合用以再生被執行正當性驗證後之資料用以執行再生處理之步驟。

127. 如申請專利範圍第126項所記載之資料處理方法，其中前述資料處理方法，

係在存儲信息核對值之核對處理中，在生成驗證對象之情形中，用以中止再生處理。

128. 一種存儲信息資料驗證試算方法，為了存儲信息資料驗證處理之存儲信息資料驗證試算方法，其特徵是：

在結合於資料驗證對象之存儲信息區段資料單位用以生成存儲信息核對值時，並再生生成後之存儲信息核對值合驗證對象存儲信息區段資料試算存儲信息資料。

129. 如申請專利範圍第128項所記載之存儲信息資料驗證試算方法，其中前述存儲信息核對值，係根據驗證對象之存儲信息區段資料合驗證信息，適用存儲信息核對值生成驗證後藉由驗證處理生成之值。

130. 如申請專利範圍第128項所記載之存儲信息資料驗證試算方法，其中前述存儲信息核對值，係根據驗證對象之存儲信息區段資料合驗證信息，適用存儲信息核對值生成驗證後藉由驗證處理生成之值。

131. 如申請專利範圍第128項所記載之存儲信息資料驗證試算方法，其中前述存儲信息核對值，係根據驗證對象之存儲信息區段資料合驗證信息，適用存儲信息核對值生成驗證後藉由驗證處理生成之值。

本公開文件係以中文書寫（CNS）A4規格（210×297mm）

六、申請專利範圍

行增裝處理生成之值。

132. 如申請專利範圍第131項所記載之存儲信息資料驗證賦予方法，其中該驗證由C/D/C模式增裝處理構成，係係在形成處理對象之信息列的一部分後經數次共同與前增裝處理適用之構成。

133. 如申請專利範圍第128項所記載之存儲信息資料驗證賦予方法，

係在存儲信息區投資資料包含有複數之零件，將該包含於該存儲信息區投資資料一部分之零件係為驗證對象時，根據驗證對象零件用以生成存儲信息驗證值，並將生成後之存儲信息驗證值與驗證對象存儲信息區投資資料予存儲信息資料。

134. 如申請專利範圍第133項所記載之存儲信息資料驗證賦予方法，其中前述存儲信息資料驗證賦予方法，

在前述存儲信息區投資資料包含有複數之零件，使驗證對象之驗證賦予零件有1個時，使對該驗證對象零件被增裝處理，藉由該驗證零件之部碼處理將該取件譯碼文全體以預定單元單位在進行部碼處理和之後，適用存儲信息驗證值生成後使用以執行增裝處理並用以生成存儲信息驗證值。

並使該驗證對象零件未經增裝處理時，將該驗證零件全體以預定單元單位將進行部碼處理和之後，適用前部存儲信息驗證值生成後用以執行增裝處理並用以生成存

本圖式是說明申請專利範圍第134項之A4圖式。(2006/2910圖)

六、申請專利範圍

儲信息驗證值，將生成後之存儲信息驗證值與驗證對象存儲信息區投資資料予存儲信息資料。

135. 如申請專利範圍第133項所記載之存儲信息資料驗證賦予方法，其中前述存儲信息資料驗證賦予方法，

係在前述存儲信息區投資資料包含有複數之零件，使驗證對象之驗證賦予零件有複數時，

在各零件適用存儲信息驗證值生成後用以執行增裝處理對該取件後之零件驗證的連結裝置，並適用前述存儲信息驗證值生成後用以執行增裝處理並適用前部結果值為存儲信息驗證值，將生成後之存儲信息驗證值與驗證對象存儲信息區投資資料予存儲信息資料。

136. 一種程式提供裝置，用以提供電腦程式由記憶庫或通訊網路提供存儲信息資料之處置在電腦裝置上執行之程式提供裝置，其特徵在於：

前述電腦程式，係包含：在包含於資料驗證對象之存儲信息區投資資料用以生成存儲信息驗證值的步驟；及藉由用以執行生成後之存儲信息驗證值的校對處理，用以執行前述資料中之存儲信息區投資資料的正常性驗證處理之步驟。

137. 一種資料處理裝置，具有使至少一部分之該被增裝處理後之複數的存儲信息區，及用以對該存儲信息區之資訊的處理部對存儲信息資料之記錄裝置用以執行生成存儲信息資料之處理的資料處理裝置。

本圖式是說明申請專利範圍第137項之A4圖式。(2006/2910圖)

六、申請專利範圍

而前述資料處理裝置，

係對前述記錄裝置形成存儲對象之存儲信息資料，將前述存儲信息區之增裝處理Kcd藉由增裝處理Kdis將進行增裝處理後之增裝處理點與Kdis [Kco]藉由進行容納則前述裝置部之資料被構成的情形中，其特徵在於其構成具有：

將前述增裝處理點資料Kdis [Keon]由前述裝置部進行取出用以執行譯碼處理並用以生成譯碼資料Kcon，而對該生成後之譯碼資料Kcon適用不同增裝處理Kstr藉由用以執行增裝處理，根據增裝處理Kstr用以生成被增裝處理後之新的增裝處理點資料並用以執行容納則前述存儲信息資料之裝置部的構成。

138. 一種資料處理裝置，具有使至少一部分之該被增裝處理後之複數的存儲信息區，及用以容納有關該存儲信息區之資訊的裝置部對存儲信息資料之記錄裝置用以執行生成存儲信息資料之處理的資料處理裝置。

而前述資料處理裝置，

係對前述記錄裝置形成包含於形成存儲對象之存儲信息資料的前述存儲信息區，藉由增裝處理Kbic被增裝處理後之存儲信息，及根據增裝處理Kco藉由被增裝處理後之增裝處理點資料Kco [Kbic]被構成，並進而，構成有關增裝處理Kco藉由增裝處理Kdis將進行增裝處理後之增裝處理點資料Kdis [Kco]容納則前述裝置部之情形中，其特徵在於其構成具有：

本圖式是說明申請專利範圍第138項之A4圖式。(2006/2910圖)

六、申請專利範圍

將前述增裝處理點資料Kdis [Keon]由前述裝置部進行取出用以執行譯碼處理並用以生成譯碼資料Kcon，而對該生成後之譯碼資料Kcon適用不同增裝處理Kstr藉由用以執行增裝處理，根據增裝處理Kstr用以生成被增裝處理後之增裝處理點資料並用以執行容納則前述存儲信息資料之裝置部的構成。

139. 一種資料處理裝置，具有使至少一部分之該被增裝處理後之複數的存儲信息區，及用以容納有關該存儲信息區之資訊的裝置部對存儲信息資料之記錄裝置用以執行生成存儲信息資料之處理的資料處理裝置。

而前述資料處理裝置，

係對前述記錄裝置形成包含於形成存儲對象之存儲信息資料的前述存儲信息區，藉由增裝處理Kbic被增裝處理後之存儲信息，及根據增裝處理Kdis藉由被增裝處理後之增裝處理點資料Kdis [Kbic]被構成之情形中，其特徵在於其構成具有：

將前述增裝處理點資料Kdis [Kbic]由前述裝置部進行取出，用以執行增裝處理Kbic譯碼處理並用以生成譯碼資料Kbic，而對該生成後之譯碼資料Kbic適用不同增裝處理Kstr藉由用以執行增裝處理，根據增裝處理Kstr用以生成被增裝處理後之增裝處理點Kstr [Kbic]並用以執行容納則存儲信息區部的構成。

140. 一種存儲信息資料生成方法，係用以生成存儲信息資料之存儲信息資料生成方法，

本圖式是說明申請專利範圍第140項之A4圖式。(2006/2910圖)

六、申請專利範圍

藉由含聲音資訊、影像資訊、程式資料至少其中之一之資料用以複數區段連結生成之存儲信息區段，

將複合於複數之存儲信息區段至少一部分之存儲信息區段藉由暗號鍵 Kcon 進行暗號處理，

將前述暗號鍵 Kcon 藉由暗號鍵 Kdis 用以生成暗號處理後之暗號鍵暗號資料 Kdis (Kcon) 並容納於前述存儲信息資料之集管部，

並用以生成含複數之存儲信息區段及集管部之存儲信息資料，

1 4 1. 如申請專利範圍第 1 4 0 項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法，係透過，

含存儲信息資料之識別資訊，

含存儲信息區段之資料長，存儲信息資料之資料範圍之識別資訊，

用以容納含前述存儲信息區段之資料長，有暗號處理後之資訊後用以生成含複數之存儲信息區段及集管部之處理，

1 4 2. 如申請專利範圍第 1 4 0 項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法，係透過，

根據構成前述集管部之一部分資訊用以生成部分暗號鍵，並將該部分暗號鍵容納於該集管部，

進而，根據前述部分暗號鍵用以生成暗號鍵暗號，並含

本國際大英法德日中國韓美專利 (CNS) A14843 (2009 2710 號)

六、申請專利範圍

將該暗號鍵暗號容納於前述集管部之處理，

1 4 3. 如申請專利範圍第 1 4 2 項所記載之存儲信息資料生成方法，其中前述部分暗號鍵之生成處理及暗號鍵暗號之生成處理，

係將前述暗號鍵暗號之資料做為信息，並將該暗號鍵暗號做為暗號鍵暗號適用 D E 5 暗號處理算法進行執行，

1 4 4. 如申請專利範圍第 1 4 1 項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法，係透過，

將前述區段資訊藉由暗號鍵 Kbit 用以暗號化處理，並將暗號鍵暗號 Kbit 藉由暗號鍵 Kdis 將生成後之暗號鍵暗號資料 Kdis (Kbit) 容納於前述集管部，

1 4 5. 如申請專利範圍第 1 4 0 項所記載之存儲信息資料生成方法，其中前述存儲信息區段中之複數區段的各區段係使用共同之固定之資料長並進行生成者，

1 4 6. 如申請專利範圍第 1 4 0 項所記載之存儲信息資料生成方法，其中前述存儲信息區段中之複數區段的各區段係使用暗號鍵暗號及暗號鍵暗號資料以規則性進行分配後做為構成並進行生成，

1 4 7. 一種存儲信息資料生成方法，用以生成存儲信息資料之存儲信息資料生成方法，

將含聲音資訊、影像資訊、程式資料至少其中之一之存儲信息區段進行複數區段連結，

將複數之存儲信息區段至少一部分之區段，將含聲音

本國際大英法德日中國韓美專利 (CNS) A14843 (2009 2710 號)

六、申請專利範圍

資訊、影像資訊、程式資料至少其中之一之資料以暗號鍵 Kbit 將進行暗號化後之暗號鍵資料部，及暗號鍵資料部之暗號鍵 Kbit 根據暗號鍵 Kcon 藉由進行暗號處理後之暗號鍵暗號資料 Kcon (Kbit) 之範圍以構成，

並將前述暗號鍵 Kcon 藉由暗號鍵 Kdis 用以生成暗號處理後之暗號鍵暗號資料 Kdis (Kcon) 並容納於前述存儲信息資料之集管部，

並用以生成含複數之存儲信息區段及集管部之存儲信息資料，

1 4 8. 一種存儲信息資料生成方法，用以生成存儲信息資料之存儲信息資料生成方法，

將含聲音資訊、影像資訊、程式資料至少其中之一之存儲信息區段進行複數區段連結，同時，

將複數之存儲信息區段至少一部分之區段，將含聲音資訊、影像資訊、程式資料至少其中之一之資料以暗號鍵 Kbit 將進行暗號化後之暗號鍵資料部，及暗號鍵資料部之暗號鍵 Kbit 根據暗號鍵 Kcon 藉由進行暗號處理後之暗號鍵暗號資料 Kdis (Kbit) 之範圍以構成，

並用以生成含複數之存儲信息區段及集管部之存儲信息資料，

1 4 9. 一種資料處理方法，具有使至少一部分之區段暗號化後之複數之存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行容納資料之處理的資料處理方法，

本國際大英法德日中國韓美專利 (CNS) A14843 (2009 2710 號)

六、申請專利範圍

對前述記錄裝置使用形成容納對象之存儲信息資料，將前述存儲信息區段之暗號鍵 Kcon 藉由暗號鍵 Kdis 將進行暗號處理後之暗號鍵暗號資料 Kdis (Kcon) 藉由容納於前述集管部後之資料被構成之資訊中，其特徵在於：

將前述暗號鍵暗號資料 Kdis (Kcon) 由前述集管部取出用以執行暗號處理並用以生成存儲資料 Kcon，

對生成後之暗號鍵暗號資料 Kcon 適用不同暗號鍵 Kstr 並藉由用以執行暗號處理，根據暗號鍵暗號 Kstr 用以生成暗號處理後之暗號鍵暗號資料 Kstr (Kcon)，

將前述生成後之暗號鍵暗號資料 Kstr (Kcon) 容納於前述存儲信息資料之集管部，並與前述複數之存儲信息區段一起容納於前述裝置，

1 5 0. 一種資料處理方法，具有使至少一部分之區段暗號化後之複數之存儲信息區段，及用以容納有關該存儲信息區段之資訊的集管部對存儲信息資料之記錄裝置用以執行容納資料之處理的資料處理方法，

係對前述記錄裝置使用形成容納對象之存儲信息資料的複數存儲信息區段，藉由暗號鍵 Kbit 將暗號化後之存儲信息，及根據暗號鍵 Kcon 藉由暗號化後之暗號鍵暗號資料 Kcon (Kbit) 被構成，進而，將暗號鍵暗號 Kcon 藉由暗號鍵 Kdis 將暗號處理後之暗號鍵暗號資料 Kdis (Kcon) 容納於前述集管部之具有構成情形中，其特徵在於：

將前述暗號鍵暗號資料 Kdis (Kbit) 由前述集管部進行

本國際大英法德日中國韓美專利 (CNS) A14843 (2009 2710 號)

六、申請專利範圍

取出用以執行譯碼處理並用以生成譯碼資料 Kcon。

而對該生成後之譯碼資料 Kcon 適用不同時鐘輸出 Kstr 藉由用以執行時鐘處理，根據時鐘輸出 Kstr 用以生成被時鐘處理後之輸出時鐘輸出資料 Kstr (Kcon)。

將前述生成後之輸出時鐘輸出資料 Kstr (Kcon) 容納到前述存儲信息資料之集管部，並將前述被輸出之存儲信息資料一起容納於前述記憶裝置。

151. 一種資料處理方法，具有使至少一部分之系統被時鐘化後之被輸出之存儲信息資料，及用以容納有關該存儲信息資料之資訊的集管部對存儲信息資料之記錄裝置用以執行容納處理的資料處理方法。

係對前述記錄裝置使包含於形成容納對象之存儲信息資料均前述存儲信息資料，藉由時鐘輸出 Kbic 被時鐘化後之存儲信息，及根據時鐘輸出 Kdis 藉由被時鐘化後之輸出時鐘輸出資料 Kdis (Kbic) 被輸出，其特徵在於：

將前述時鐘輸出資料 Kdis (Kbic) 由前述集管部進行輸出，用以執行該時鐘輸出 Kbic 譯碼處理並用以生成譯碼資料 Kbic。

而對該生成後之譯碼資料 Kbic 適用不同時鐘輸出 Kstr 藉由用以執行時鐘處理，根據時鐘輸出 Kstr 用以生成被時鐘處理後之輸出時鐘輸出 Kstr (Kbic)。

將前述生成後之輸出時鐘輸出資料 Kstr (Kbic) 容納到存儲信息資料，並與被輸出之存儲信息資料一起容納於前述記憶裝置。

本局人員建議用中國國家知识产权局 (CN) AI 號碼 [20072770]。

-311-

六、申請專利範圍

152. 一種程序提供裝置，用以提供電腦程式具有使至少一部分之系統被時鐘化後之被輸出之存儲信息資料，及用以容納有關該存儲信息資料之資訊的集管部對存儲信息資料之記錄裝置容納資料之生成處理在電腦系統執行之程式提供裝置，而前述電腦程式。

係對前述記錄裝置使包含於容納對象之存儲信息資料，將前述存儲信息資料之輸出時鐘輸出 Kcon 藉由時鐘輸出 Kdis 將該輸出時鐘化後之輸出時鐘輸出資料 Kdis (Kcon) 藉由前述集管部之資料被輸出，其特徵在於：

將前述時鐘輸出資料 Kdis (Kbic) 由前述集管部進行輸出用以執行譯碼處理並用以生成譯碼資料 Kcon 之步驟。

而對該生成後之譯碼資料 Kcon 適用不同時鐘輸出 Kstr 藉由用以執行時鐘處理，根據時鐘輸出 Kstr 用以生成被時鐘處理後之輸出時鐘輸出 Kstr (Kcon) 之步驟。

將前述生成後之輸出時鐘輸出資料 Kstr (Kcon) 容納到前述存儲信息資料之集管部之步驟。

153. 一種資料處理裝置，藉由記憶裝置或通訊裝置進行被輸出之存儲信息資料之可生處理之資料處理裝置，其特徵在於：

存儲信息資料解析部，含被輸出後之存儲信息資料及該輸出後之存儲信息資料之仲長處理裝置用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之輸出後之存儲信息資料，及仲長處理裝置之仲長處理；及

仲長處理部，係為前述存儲信息資料解析部之解析部。

本局人員建議用中國國家知识产权局 (CN) AI 號碼 [20072770]。

-312-

六、申請專利範圍

其使用被包含於被輸出後之存儲信息資料之仲長處理裝置用以執行被包含於該存儲信息資料之輸出後之存儲信息資料之仲長處理。

154. 如申請專利範圍第 153 項所記載之資料處理裝置，其中資料處理裝置，係進行具有：

資料記憶部，藉由前述存儲信息資料解析部用以容納輸出後之輸出後之存儲信息；及

仲長處理部，藉由前述存儲信息資料解析部用以容納輸出後之仲長處理裝置。

而前述仲長處理裝置，係對被記憶於前述資料記憶部後之輸出後之存儲信息，適用被記憶於前述仲長處理裝置之仲長處理裝置並用以執行仲長處理。

155. 如申請專利範圍第 153 項所記載之資料處理裝置，其中前述存儲信息資料解析部其構成部。

該裝置包含於前述存儲信息資料之集管部用以容納存儲信息資料之構成裝置並進行存儲信息資料之解析。

156. 如申請專利範圍第 155 項所記載之資料處理裝置，其中在前述集管部。

係包含輸出後之存儲信息之仲長處理裝置。

該仲長處理裝置中使仲長處理裝置對象之輸出後之存儲信息有數個。

則前述仲長處理裝置，係在該仲長處理裝置中使仲長處理裝置對象之輸出後之存儲信息中，係使該仲長處理裝置對象之輸出後之存儲信息。

本局人員建議用中國國家知识产权局 (CN) AI 號碼 [20072770]。

-313-

六、申請專利範圍

位用以執行順序存儲信息仲長處理之構成。

157. 如申請專利範圍第 153 項所記載之資料處理裝置，其中前述資料處理裝置，係進行具有：

顯示裝置，用以顯示形成仲長處理對象之輸出後之存儲信息之資訊；及

輸入裝置，由該裝置於前述仲長處理後之存儲信息資料用以輸入被該裝置之仲長處理之仲長處理裝置。

係由前述輸入裝置根據被輸入後之仲長處理裝置之資訊，用以執行對應於該資訊之輸出後之存儲信息之仲長處理之構成。

158. 一種資料處理裝置，藉由記憶裝置或通訊裝置進行被輸出之存儲信息資料之可生處理之資料處理裝置，其特徵在於：

用以接收輸出後之存儲信息，其仲長處理裝置其中之一之存儲信息資料，由該裝置接收存儲信息資料之集管部用以該存儲信息資料用以判斷輸出後之存儲信息或仲長處理裝置，同時

使該存儲信息資料有關輸出後之存儲信息資料之集管部，用以取得被輸出於該輸出後之存儲信息或仲長處理裝置，並具有：

存儲信息資料解析部，使該存儲信息資料具有仲長處理裝置時，由該存儲信息資料之集管部用以取得仲長處理裝置之構成；及

仲長處理部，係為前述存儲信息資料解析部之解析部。

本局人員建議用中國國家知识产权局 (CN) AI 號碼 [20072770]。

-314-

六、申請專利範圍

仲長處理部，用以執行壓縮存儲信息之仲長處理；
而前述仲長處理部，其構造具有：

使前述存儲信息資料解析部所接之壓縮存儲信息之壓縮處理程式種類將可適用之仲長處理程式，藉由前述存儲信息資料解析部根據該解碼後之仲長處理程式種類進行選擇，藉由該選擇後之仲長處理程式用以執行仲長處理。

159. 如申請專利範圍第158項所記載之資料處理裝置，其中前述資料處理裝置，係進而具有：

資料記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之壓縮存儲信息；及

程式記憶部，藉由前述存儲信息資料解析部用以容納被抽出後之仲長處理程式；

而前述仲長處理部，係對被記憶於前述資料記憶部後之壓縮存儲信息，適用被記憶於前述程式記憶部後之仲長處理程式以仲長處理之構成。

160. 如申請專利範圍第158項所記載之資料處理裝置，其中在前述裝置資訊，

係被壓縮存儲信息之再生優先順位資訊，使形成仲長處理對象之壓縮存儲信息有被解碼。

而在前述仲長處理部中之存儲信息仲長處理部，係在前述存儲信息資料解析部中根據被抽取後之無管理資訊中之優先順位資訊，依從該優先順位進行執行順序之構成。

161. 如申請專利範圍第158項所記載之資料處理

本表以A1或A4格式申請專利權 (CNS) A4格式 (30X30X30)

-315-

六、申請專利範圍

裝置，其中前述資料處理裝置，

係具有檢索裝置用以檢索仲長處理程式，

而前述裝置裝置，

係對解碼而進存儲信息資料解析部後之壓縮存儲信息種類將可適用之仲長處理程式，使前述資料處理裝置將可存取之程式容納裝置做為檢索對象進行檢索之構成。

162. 如申請專利範圍第158項所記載之資料處理裝置，其中前述資料處理裝置，係進而具有：

顯示裝置，用以顯示形成仲長處理對象之壓縮存儲信息的資訊；及

輸入裝置，由該顯示於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；

而前述仲長處理部，

係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的仲長處理之構成。

163. 一種資料處理方法，係藉由記憶媒體或通訊媒體進行被提供之存儲信息資料之再生處理之資料處理方法，其特徵係具有：

存儲信息資料解析步驟，含被壓縮後之存儲信息及其壓縮存儲信息之仲長處理程式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之壓縮存儲信息，及仲長處理程式之抽出處理；及

仲長處理步驟，係為前述存儲信息資料解析之解析結

本表以A1或A4格式申請專利權 (CNS) A4格式 (30X30X30)

-316-

六、申請專利範圍

果使用該合於被抽取後之存儲信息資料之仲長處理程式用以執行該合於該存儲信息資料之壓縮存儲信息的仲長處理。

164. 如申請專利範圍第163項所記載之資料處理方法，其中前述資料處理方法，係進而具有：

資料記憶步驟，藉由前述存儲信息資料解析步驟用以容納被抽出後之壓縮存儲信息；及

程式記憶步驟，藉由前述存儲信息資料解析部用以容納被抽出後之仲長處理程式；

而前述仲長處理步驟，係對被記憶於前述資料記憶部後之壓縮存儲信息，在前述被記憶於前述資料記憶部後之仲長處理程式並用以執行仲長處理之構成。

165. 如申請專利範圍第163項所記載之資料處理方法，其中在前述裝置資訊，

係根據被合於前述存儲信息資料之無管理資訊以取得存儲信息資料之構成資訊並進行存儲信息資料之解析。

166. 如申請專利範圍第165項所記載之資料處理方法，其中在前述無管理資訊，

係被含壓縮存儲信息之再生優先順位資訊，

在前述仲長處理部中形成仲長處理對象之壓縮存儲信息與被抽取時。

而前述仲長處理步驟，

係在前述存儲信息資料解析步驟中根據被抽取後之無管理資訊中之優先順位資訊，依從該優先順位以執行順序

本表以A1或A4格式申請專利權 (CNS) A4格式 (30X30X30)

-317-

六、申請專利範圍

存儲信息仲長處理。

167. 如申請專利範圍第163項所記載之資料處理方法，其中前述資料處理方法，係進而具有：

顯示步驟，將該合於前述被抽出後之壓縮存儲信息的資訊顯示於顯示裝置；及

輸入步驟，由該顯示於前述顯示裝置後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；

而前述仲長處理步驟，

係由前述輸入步驟根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之壓縮存儲信息的仲長處理。

168. 一種資料處理方法，藉由記憶媒體或通訊媒體進行被提供之存儲信息資料之再生處理之資料處理方法，其特徵在於：

用以檢索含壓縮存儲信息，或仲長處理程式其中之一之存儲信息資料，由該檢索而取得存儲信息資料之構成資訊以取得存儲信息資料用以執行存儲信息資料之再生處理之資料處理方法，同時

使該存儲信息資料有壓縮存儲信息時，由該存儲信息資料之無管理資訊，用以取得被記憶於該壓縮存儲信息後之壓縮處理程式，茲具有：

存儲信息資料解析步驟，使該存儲信息資料有仲長處理程式時，由該存儲信息資料之無管理資訊以取得仲長處理程式之構成；

本表以A1或A4格式申請專利權 (CNS) A4格式 (30X30X30)

-318-

六、申請專利範圍

選擇步驟，在前述存儲信息資料解析步驟中對解析後之應儲存信息的應輸出處理程序類型將可適用之仲長處理程式，藉由前述存儲信息資料解析步驟繼續被解析後之仲長處理程式繼續加以選擇；及

仲長處理步驟，在前述選擇步驟中藉由選擇後之仲長處理程式用以執行仲長處理。

169. 如申請專利範圍第168項所記載之資料處理方法，其中前述資料處理方法，係進而具有：

資料記憶步驟，藉由前述存儲信息資料解析部用以將前述輸出後之應儲存信息；及

程式記憶步驟，藉由前述存儲信息資料解析部用以將前述輸出後之仲長處理程式；

而前述仲長處理步驟，

係在前述資料記憶步驟對被記憶後之應儲存信息，並前述程式記憶步驟中適用被記憶後之仲長處理程式並用以仲長處理。

170. 如申請專利範圍第168項所記載之資料處理方法，其中在前述應儲存信息，

係將應儲存信息之再生優先順位資訊，假形成仲長處理對象之應儲存信息有被暫時，

則在前述仲長處理步驟，

係在前述存儲信息資料解析步驟中根據被取得後之應儲存資訊中的優先順位資訊，使該應優先順位進行順序執行。

本申請案係以美國專利局第7,210,270號專利為準

-319-

六、申請專利範圍

171. 如申請專利範圍第168項所記載之資料處理方法，其中前述資料處理方法，係進而具有：

檢查步驟用以檢查仲長處理程式。

而前述檢查步驟，

係在前述存儲信息資料解析步驟中對進行解析後之應儲存信息種類將可適用之仲長處理程式，將可存取之程式資訊與應被檢查對象之應儲存信息之資訊類比於顯示表；及

172. 如申請專利範圍第168項所記載之資料處理方法，其中前述資料處理方法，係進而具有：

顯示步驟，係將前述處理對象之應儲存信息的資訊類比於顯示表；及

輸入步驟，由該顯示表對該顯示表後之存儲信息資訊用以輸入被選擇後之再生存儲信息識別資料；

而前述仲長處理步驟，

係由前述輸入裝置根據被輸入後之再生存儲信息識別資料，用以執行對應於該識別資料之應儲存信息的仲長處理。

173. 一種存儲信息資料生成方法，藉由記憶媒體或通訊媒體進行提供之存儲信息資料的生成處理之存儲信息資料生成方法，其特徵為：

用以生成被記憶媒體之存儲信息及該應儲存信息之仲長處理程式組合的存儲信息資料。

174. 如申請專利範圍第173項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進

本申請案係以美國專利局第7,210,270號專利為準

-320-

六、申請專利範圍

而，

做為前述存儲信息資料之應儲存資訊用以前述存儲信息資料之構成資訊。

175. 如申請專利範圍第173項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進而，

做為前述存儲信息資料之應儲存資訊，係用以附加被含於該存儲信息資料之存儲信息的再生優先順位資訊。

176. 一種存儲信息資料生成方法，係藉由記憶媒體或通訊媒體進行提供之存儲信息資料的生成處理之存儲信息資料生成方法，其特徵為：

使存儲信息資料將用以識別被應儲存信息或仲長處理程式之存儲信息資料繼續提供為應儲存資訊進行附加。

使該存儲信息資料係應儲存信息時，則將被適用於該應儲存信息後之應輸出處理程序繼續提供為應儲存資訊進行附加。

而使該存儲信息資料係仲長處理程式時，則將仲長處理程式繼續提供為應儲存資訊並用以生成進行附加後之存儲信息資料。

177. 如申請專利範圍第176項所記載之存儲信息資料生成方法，其中前述存儲信息資料生成方法中，進而，

做為前述存儲信息資料之應儲存資訊，係用以附加被含於該存儲信息資料之存儲信息的再生優先順位資訊。

本申請案係以美國專利局第7,210,270號專利為準

-321-

六、申請專利範圍

178. 一種提供媒體，用以提供電腦程式藉由記憶媒體或通訊媒體將被提供存儲信息資料之再生處理在電腦系統上執行的程式提供媒體，其特徵在於：前述電腦程式，係具有：

存儲信息資料解析步驟，含被解析後之存儲信息及該應儲存信息之仲長處理程式用以執行存儲信息資料之存儲信息資料解析，並用以執行由該存儲信息資料之應儲存信息，及仲長處理程式之輸出處理；及

仲長處理步驟，做為前述存儲信息資料之解析結果使用基於該被取得後之存儲信息資料的仲長處理程式用以執行被含於該存儲信息資料之應儲存信息的仲長處理。

本申請案係以美國專利局第7,210,270號專利為準

-322-

第5圖

無管板機
存儲信息模塊
格式型式
格式型號
存儲信息型號
信息優先輸出資訊
限制利用資訊
限制存取資訊
限制存取資訊
加密算法
加密化模式
驗證方法

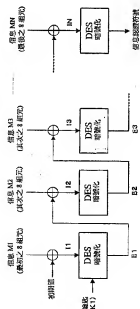
處理方針

第6圖

存儲信息模塊	
置換模塊	
置換 I	置換化模塊
	置換對象資訊
	存儲信息模塊
置換模塊	
置換 N	置換化模塊
	置換對象資訊
	存儲信息模塊

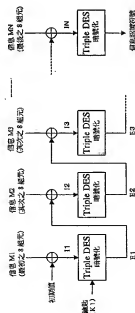
置換資訊

第7圖

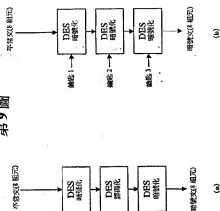


⊕ 排他性邏輯和(異或)單元

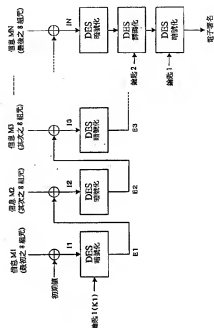
第8圖



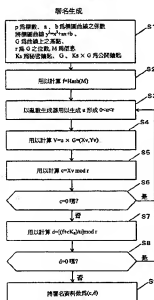
第9圖



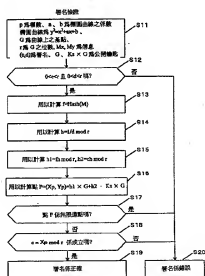
第10圖



第 11 圖



第 12 圖



第 13 圖

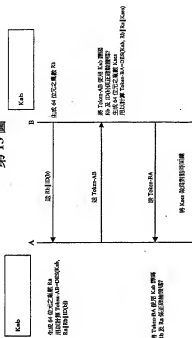
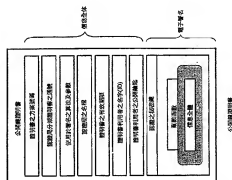


圖 13 顯示了 A 和 B 之間的公鑰交換過程。

第 14 圖



第 15 圖

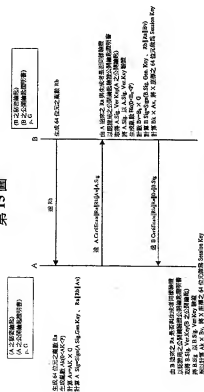
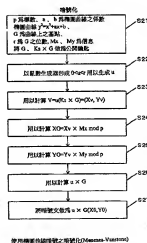
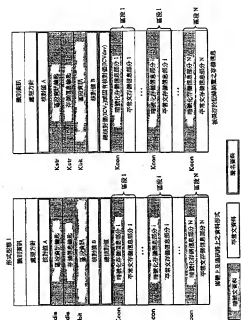


圖 15 顯示了 A 和 B 之間的公鑰交換過程。

第 16 圖

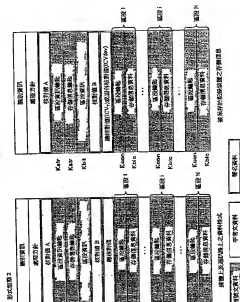


第 33 圖



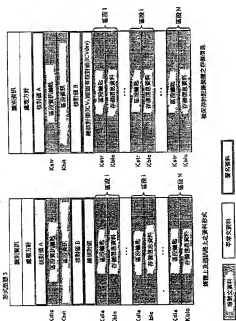
188

第 34 圖



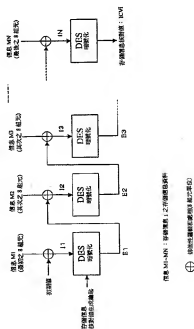
189

第 35 圖

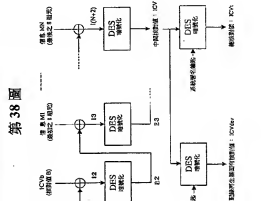
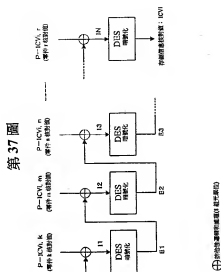


190

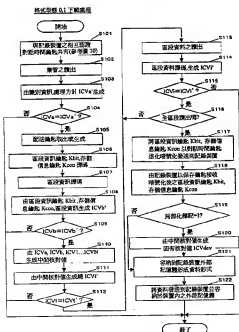
第 36 圖



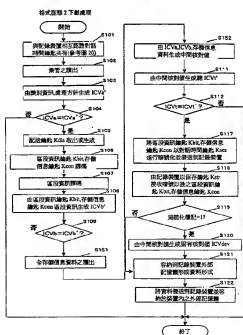
191



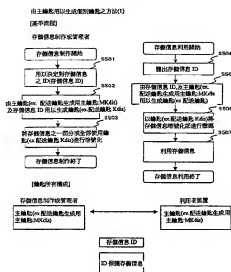
第39圖



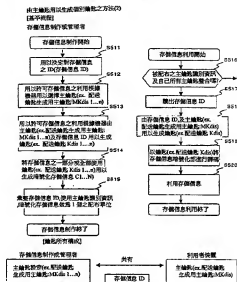
第40圖



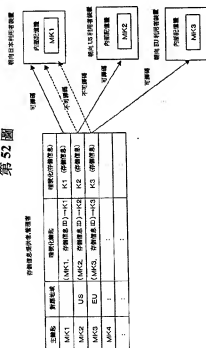
第 50 圖



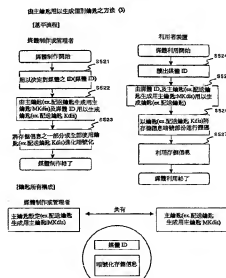
第 51 圖



第52圖

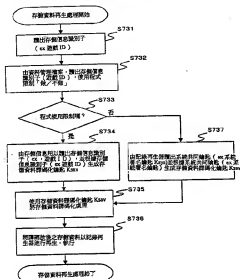


第 53 圖

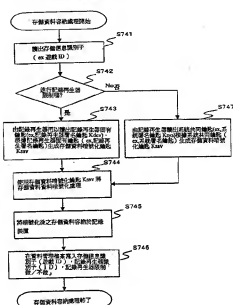


第 74 圖

(4) 使用存儲單元 ID 系統內附編碼之存儲資料再生處理系列



第 75 圖

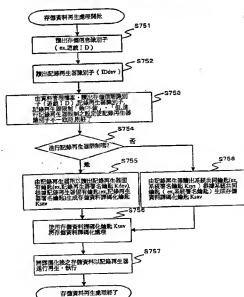
(5) 使用存儲單元全部附編碼，ex. 系統內附編碼
之存儲資料再生處理系列

第 76 圖

資料名稱	存儲單元識別字 (邏輯 ID)	存儲單元識別字 (邏輯 ID)	存儲單元識別字 (邏輯 ID)
1	12345678...	56789012...	89012345...
2	ABCDEF12...	09876543...	34567890...
3	12345678...	56789012...	89012345...

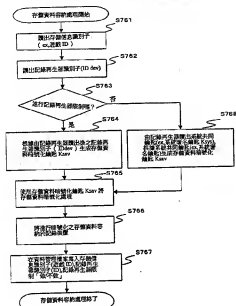
第 77 圖

(6) 使用存儲單元全部附編碼，ex. 系統內附編碼之存儲資料再生處理系列



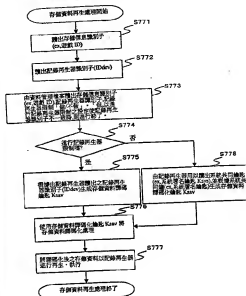
第78圖

(7) 使用記錄再生磁帶磁頭，或系統不同磁頭之存儲資料控制處理例

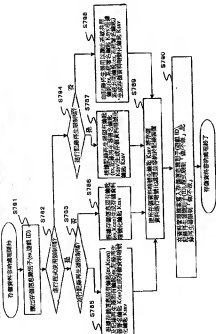


第 79 圖

(四) 應用記憶再生原理到平、近系統共同
編製之存儲資料再生處理例



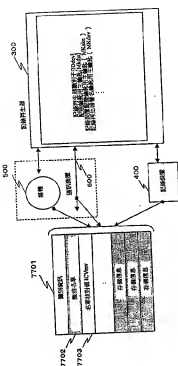
第80圖

[illegible]

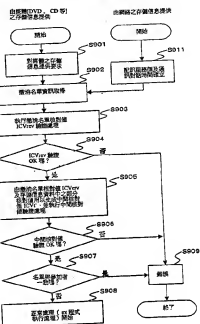
第81圖

新到號碼	存貨號碼(字號) 品名	存貨數量(字號) 單位	正式出庫日期	出庫地點(字號)
1	12345678..	45678901..	無	存庫
2	ABCDEF12..	9876543..	無	無
3	12345678..	5432109..	有庫	無
4

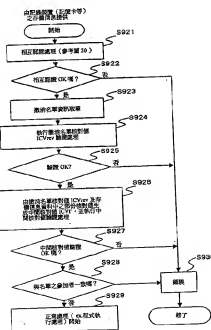
第 86 圖



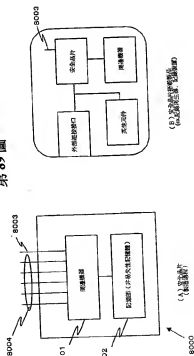
第 87 圖



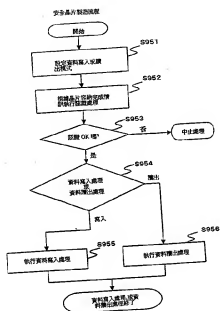
第 88 圖



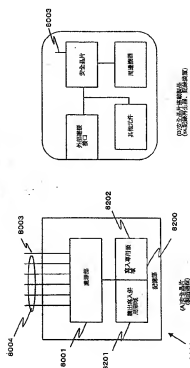
第 89 圖



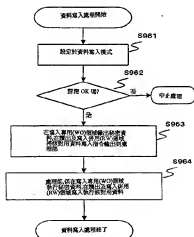
第 90 圖



第 91 圖



第 92 圖



第 93 圖

